

Exhibit 11

KuCoin Hack

Saturday, July 13, 2024 10:08 PM

On September 25, 2020, KuCoin announced on their website that they were hacked:



Dear KuCoin Users,

We detected some large withdrawals since September 26, 2020 at 03:05:37 (UTC+8). According to the latest internal security audit report, part of Bitcoin, ERC-20 and other tokens in KuCoin's hot wallets were transferred out of the exchange, which contained few parts of our total assets holdings. The assets in our cold wallets are safe and unharmed, and hot wallets have been re-deployed.

We are locating the reason for the incident, and will keep you updated once it is confirmed. **Please rest assured that if any user fund is affected by this incident, it will be covered completely by KuCoin and our insurance fund.**

The next day, they posted an update with additional details:

kucoin.com/announcement/en-kucoin-ceo-livestream-recap-l...

KUCCOIN Buy Crypto Markets Trade Derivatives Earn Institutional More

Home / Announcements / KuCoin CEO Livestream Recap - Latest Updates About Security Incident

KuCoin CEO Livestream Recap - Latest Updates About Security Incident

09/26/2020, 03:56:54



In response to the recent KuCoin Security Incident, KuCoin Global CEO Johnny Lyu hosted a livestream at 12:30 (UTC+8) on September 26, 2020, and announced more updates regarding the incident.

He mentioned that, according to the latest internal security audit report, part of the Bitcoin, ERC-20 and other tokens in KuCoin's hot wallets were transferred out of the exchange, which contained few parts of the total assets holdings. The assets in the cold wallets are safe and unharmed, and the hot wallets have been re-deployed.

We are locating the reason for the incident, and will keep users updated once it is confirmed. **Please rest assured that if any user fund is affected by this incident, it will be covered completely by KuCoin and our insurance fund.**

Here's the recap of the livestream.

Johnny first explained the timeline of the incident as below:

In this announcement, KuCoin stated that the hacker's wallet address was 0xeb31...8c23:

kucoin.com/announcement/en-kucoin-ceo-livestream-recap-l...

KUCCOIN Buy Crypto Markets Trade Derivatives Earn Institutional More Log

Then, a few more abnormal transactions for ETH and other ERC-20 tokens were monitored:

0x56fd1c3c8cc861c8abceafac7a175ccfb53bb87877750b0bfd9581d8c52c1bc

0x57e205922325104f9d132ff7cddb7eb94bfe15049b5c71cb7328f72bc69a7122

0xd2b21c8bb5c0bfafc98e86a2e924f3fe4223356748486bdcccd8bf58e16aa93

0xdf1f8ce5d491728a2573591b253e2a9ec6abda723c7d984af1f6f154cd231ed9

0xc3bd740534a530cfa5060daf937a24c5c90b1783550c6d9fa61daa2c1873e734

0x5bf11bd22b653870c1ba8cad69ae0691e08d9f73762a5adfc9e37f1892d9eee

And all abnormal transactions are from this wallet address: 0xeb31973e0feb3e3d7058234a5ebbae1ab4b8c23

At 03:01 AM (UTC+8) on September 26, 2020, we received an alert from the risk management system regarding the abnormal remaining balance of our hot wallets.

At 03:15 AM (UTC+8) on September 26, 2020, the KuCoin team set up a special team to cope with the incident.

At 03:20 AM (UTC+8) on September 26, 2020, the KuCoin operation team urgently closed the server of the wallet and found that after the shutdown, there were still cases of abnormal transactions.

Using Etherscan, I can see the four transactions that where the KuCoin hacker transferred approximately 11,486 ETH (\$4.04 mm) :

Axie Infinity

Sunday, July 14, 2024 10:22 PM

On March 29, 2022, Ronin announced on their blog roninchain.com/blog that Ronin bridge had been hacked for 173,600 ETH and 25,500,000 USDC. The blog post details the two malicious transaction and it reveals the destination wallet of the stolen funds: 0x098b716b8aaf21512996dc57eb0615e2383e2f96

Where are the funds now?

Most of the hacked funds are still in the hacker's wallet:
<https://etherscan.io/address/0x098b716b8aaf21512996dc57eb0615e2383e2f96>

How did this happen?

We are in the process of conducting a thorough investigation.

Five validator private keys were hacked; 4 Sky Mavis validators and 1 Axie DAO.

The validator key scheme is set up to be decentralized so that it limits an attack vector such as this, but the attacker found a backdoor through our gas-free RPC node, which they abused to get the signature for the Axie DAO validator.

This traces back to November 2021 when the Axie DAO validator was allowlisted to distribute free transactions. This was discontinued in December 2021, but the Axie DAO validator IP was still on the allowlist.

Here is the transaction showing the 173,600 ETH moving to the hacker's wallet on 03/23/2022:

Address: 0x098b716b8aaf21512996dc57eb0615e2383e2f96

Overview

ETH BALANCE: 101.80192993376705535 ETH
 ETH VALUE: \$336,322.53 (@ \$3,303.69/ETH)
 TOKEN HOLDINGS: \$4.62 (23 Tokens)

More Info

PRIVATE NAME TAGS: + Add
 LAST TXN SENT: 0xc10b3487dc4... from 481 days ago
 FIRST TXN SENT: 0xc28fad5ebd5... from 844 days ago

Multichain Info

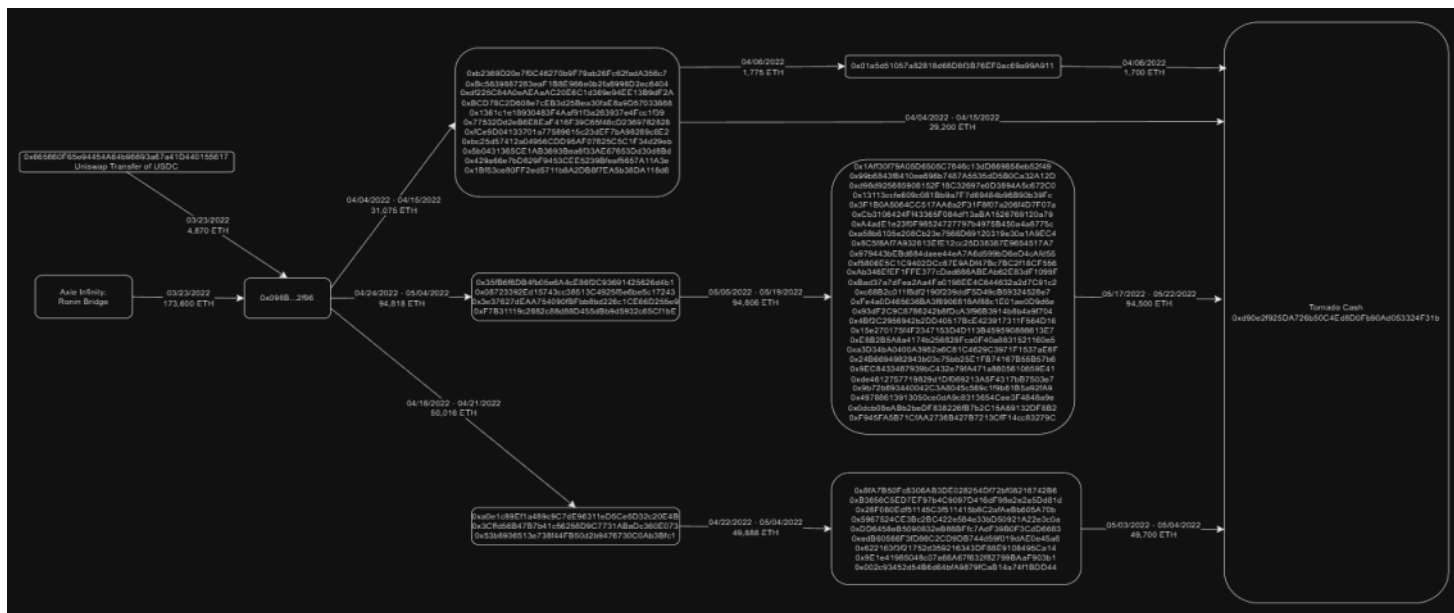
\$336,350.87 (Multichain Portfolio)
 2 addresses found via Blockscan

Transactions | Internal Transactions | Token Transfers (ERC-20) | NFT Transfers | Analytics | Multichain Portfolio | Cards

Latest 2 Internal transactions

Parent Transaction Hash	Block	Date Time (UTC)	From	To	Amount
0xc0b122e195d...	18263472	2023-10-16 14:15:59	Sorare: Withdrawal	Ronin Bridge Exploiter	0.0001 ETH
0xc28fad5ebd5...	14442835	2022-03-23 13:29:09	Axie Infinity: Ronin Brid...	Ronin Bridge Exploiter	173,600 ETH


The stolen 173,600 ETH was combined with 4,870 ETH that was swapped for Tether. The ETH was moved through a series of intermediary wallets between 04/04/2022 and 05/19/2022. Between 04/04/2022 and 05/22/2022, 175,100 ETH was transferred to Tornado Cash. The total amount transferred to Tornado Cash was approximately \$449.0 million.







Origin Protocol


Tuesday, September 10, 2024 6:44 PM


On 11/17/2020, Mathew Liu the cofounder of Origin Protocol announced on Origin's blog at [medium.com/@matthewliu/](https://medium.com/@matthewliu/urgent-ousd-has-hacked-and-there-has-been-a-loss-of-funds-7b8c4a7d534c) that the Origin Dollar had been hacked and that value was stolen by Ethereum address `0xb77f7bbac3264ae7abc8aedf2ec5f4e7ca079f83`.














medium.com/@matthewliu/urgent-ousd-has-hacked-and-there-has-been-a-loss-of-funds-7b8c4a7d534c




 Get unlimited access to the best of Medium for less than \$1/week. [Become a member](#)

Urgent: OUSD Was Hacked and There Has Been a Loss of Funds


 Matthew Liu · Follow
 12 min read · Nov 16, 2020

 670
  8
 



OUSD has been hacked, and there has been a loss of user funds. We are actively investigating the issue. We are committed to making things right. Please refer to this blog post as the authoritative source for continual updates over the course of the next few days.

Updated at 1:00AM UTC 12.12.2020 (Matthew Liu)



We have now published our [compensation plan](#) in full detail. If you are an affected user, please refer to that post.

Updated at 10:26AM UTC 11.25.2020 (Josh Fraser)

We want to share a rough timeline on when to expect full details regarding the compensation plan for the OUSD hack. Our current estimate is that it will take about 2 weeks to have a plan ready to share. It may take longer, but we hope to get it done faster. In approximately 2 weeks, we expect to be able to share our proposal for when and how affected parties will be reimbursed. The actual reimbursement will then happen at a later time. There are a lot of varying situations that we are trying to understand, so that we can structure a proposal that is fair to everyone. For example, we are collecting and analyzing data to understand how many people fall into each of the following categories:

- Users that have held OUSD in their wallets since the attack
- Liquidity providers on SushiSwap, Uniswap, or Mooniswap
- SnowSwap stakers

Here is the part specifically mentioning where the stolen value was transferred:



medium.com/@matthewliu/urgent-ousd-has-hacked-and-there-has-been-a-loss-of-funds-7b8c4a7d534c

Updated at 10:38 AM UTC 11.17.2020 (Micah Alcorn)

As promised in an earlier update, we wanted to provide a detailed walk-through of the attack on the OUSD vault that happened earlier today. We'll follow up with a full post-mortem in the coming days to explore a variety of ways to prevent future attacks. For now, we want to quickly shed light on what happened.

We will also have an upcoming post discussing the latest on our efforts to recover funds as well as our worst-case scenario plans to compensate users if we're unable to recoup user deposits.

The attack originated from `0xb77f7bbac3264ae7abc8aedf2ec5f4e7ca079f83`, with a [contract](#) deployed at Nov-17-2020 12:40:56 AM +UTC. Here is a description of the transactions that were initiated by this contract:

• • •

Nov-17-2020 12:47:19 AM +UTC

Nov-17-2020 12:47:19 AM +UTC

1. The Flash Loan

70,000 ETH was borrowed from dYdX.

2. The Stablecoin Swaps

17,500 ETH was exchanged for 7,855,911.53 USDT on Uniswap.

52,500 ETH was exchanged for 20,987,772.08 DAI on Uniswap.

3. The Simple Mint

Our mint method, which allows the sender to use one type of stablecoin to mint OUSD, was called with 7,500,000 USDT.

7,500,000 USDT was transferred to the vault.

7,500,000 OUSD was minted and transferred to the attacker, as intended.

An analysis of the malicious contract shows the attacker manipulating and withdrawing funds from Origin as described in the blog post:

ETH Price: \$2,390.29 (+1.28%) Gas: 4.478 Gwei

Search by Address / Txn Hash / Block / Token / Domain Name

Etherscan

Home Blockchain Tokens NFTs Resources Developers More Sign In

Token Transfers (ERC-20)

For 0x47c3d8439d043a4f42f6422acc27bb7240fde2

Sponsored: MetaWin: Complete for your share of \$ 1 MILLION in prizes. \$350k for 1st Place. Play Now!

Transactions involving tokens marked as suspicious, unsafe, spam or brand infringement are currently hidden. To show them, go to Site Settings.

Transactions with zero token value are currently hidden. To show them, please go to Site Settings.

A total of 93 txns found

Download Page Data First < Page 1 of 1 > Last

Transaction Hash	Method	Block	Date Time (UTC)	From	To	Amount	Token
0x2c9d20292e...	0x7db4e34811...	11272312	2020-11-17 1:01:08	0x47C3d843...7240FDFE2	Origin: Deployer	498,487.663713097	Origin Dolla... (OUSD)
0x7db4e34811...	Collect	11272305	2020-11-17 0:59:48	0x47C3d843...7240FDFE2	0xb77f78BA...7cA079F83	121,577.536437652	Dai Stableco... (DAI)
0x7db4e34811...	Collect	11272305	2020-11-17 0:59:48	0x47C3d843...7240FDFE2	Uniswap V2: USDC	24,443.075929	USDC (USDC)
0x7db4e34811...	Collect	11272305	2020-11-17 0:59:48	0x47C3d843...7240FDFE2	Uniswap V2: USDT	434,407.947703	Tether USD (USDT)
0x9a133457d8...	Redeem	11272303	2020-11-17 0:59:43	0x47C3d843...7240FDFE2	Null: 0x000...000	4,714.705009138	Origin Dolla... (OUSD)
0x9a133457d8...	Redeem	11272303	2020-11-17 0:59:43	Origin Dollar: DAI Com...	0x47C3d843...7240FDFE2	557.826941	USDC (USDC)
0x9a133457d8...	Redeem	11272303	2020-11-17 0:59:43	Origin Dollar: DAI Com...	0x47C3d843...7240FDFE2	1,336.096992	Tether USD (USDT)
0x9a133457d8...	Redeem	11272303	2020-11-17 0:59:43	Origin Dollar: DAI Aave ...	0x47C3d843...7240FDFE2	2,774.577896887	Dai Stableco... (DAI)
0x9a133457d8...	Redeem	11272303	2020-11-17 0:59:43	0x47C3d843...7240FDFE2	Null: 0x000...000	6,901.561743508	Origin Dolla... (OUSD)
0x9a133457d8...	Redeem	11272303	2020-11-17 0:59:43	Origin Dollar: DAI Com...	0x47C3d843...7240FDFE2	816.567934	USDC (USDC)
0x9a133457d8...	Redeem	11272303	2020-11-17 0:59:43	Origin Dollar: DAI Com...	0x47C3d843...7240FDFE2	1,955.828702	Tether USD (USDT)
0x9a133457d8...	Redeem	11272303	2020-11-17 0:59:43	Origin Dollar: DAI Aave ...	0x47C3d843...7240FDFE2	4,061.531163906	Dai Stableco... (DAI)
0x8eba96d3f58...	0xa2607Add	11272293	2020-11-17 0:57:07	SushiSwap: OUSD-USDT	0x47C3d843...7240FDFE2	98,401.287261	Tether USD (USDT)
0x8eba96d3f58...	0xa2607Add	11272293	2020-11-17 0:57:07	0x47C3d843...7240FDFE2	SushiSwap: OUSD-USDT	1,000,000	Origin Dolla... (OUSD)
0x8eba96d3f58...	0xa2607Add	11272293	2020-11-17 0:57:07	Uniswap V2: OUSD-US...	0x47C3d843...7240FDFE2	29,803.079523	Tether USD (USDT)

Tornado Cash Page 23

Compounder Finance

Wednesday, September 11, 2024 10:45 AM

Compounder.finance was a rug pull scam that began on 11/29/2020 that was widely reported in the crypto press.

Their website no longer exists, but I found it using archive.org.

Click to connect your wallet
Placeholder

COMPOUNDER.FINANCE

Token 1 Token 2 Token 3 Token 4 Token 5
Twitter Sigele Github Etherscan Uniswap Discord Telegram

Assets Under Management:
- USD
DAO Treasury:
- USD
CP3R Price: - USD
Your CP3R Balance: -
Market cap: - USD
Circulating Supply: -
Smarter Farming: Earn compounding interest on your deposited asset & SCP3R rewards W/ 0% IL, 24-HOUR TIMELOCK ON CONTRACTS AND NEW POOLS INCOMING
Enable private withdraw: Coming Soon™

Asset	Staked Balance	Apv	Strategy	Earned Amount	Deposit	Withdraw
CP3R-ETH LP CP3R-ETH LP Get LP Token	-	-	Placeholder LP TOKEN: 0.30% Placeholder CP3R REWARDS: -%	0.000	Approve Deposit	MAX
CP3R CP3R Buy CP3R	-	-	CP3R Emissions CP3R REWARDS: -%	0.000	Approve Deposit	MAX
WBTC WBTC	-	-	Placeholder Compound: -% Placeholder CP3R REWARDS: -%	0.000	Approve Deposit	MAX
Ethereum WETH	-	-	Placeholder CP3R REWARDS: -%	0.000	Approve Deposit	MAX
DAI DAI	-	-	Placeholder CURVE: -% Placeholder CP3R REWARDS: -%	0.000	Approve Deposit	MAX
Tether USDT	-	-	Placeholder COMPOUND: -% Placeholder CP3R REWARDS: -%	0.000	Approve Deposit	MAX
USDC USDC	-	-	Placeholder COMPOUND: -% Placeholder CP3R REWARDS: -%	0.000	Approve Deposit	MAX
YFI YFI	-	-	Placeholder YFI Governance: -% Placeholder CP3R REWARDS: -%	0.000	Approve Deposit	MAX
UNI UNI	-	-	Placeholder Compound: -% Placeholder CP3R REWARDS: -%	0.000	Approve Deposit	MAX
Placeholder COMPOUNDER.FINANCE						

The etherscan link on their webpage shows that the compounder.finance Ethereum address is: 0x7ef1081ecc8b5b130656a41d4ce4f89dbbcc8c

Click to connect your wallet
Placeholder

COMPOUNDER.FINANCE

Token 1 Token 2 Token 3 Token 4 Token 5
Twitter Sigele Github Etherscan Uniswap Discord Telegram

Assets Under Management:
- USD
DAO Treasury:
- USD
CP3R Price: - USD
Your CP3R Balance: -
Market cap: - USD
Circulating Supply: -
Smarter Farming: Earn compounding interest on your deposited asset & SCP3R rewards W/ 0% IL, 24-HOUR TIMELOCK ON CONTRACTS AND NEW POOLS INCOMING
Enable private withdraw: Coming Soon™

Asset	Staked Balance	Apv	Strategy	Earned Amount	Deposit	Withdraw
CP3R-ETH LP CP3R-ETH LP Get LP Token	-	-	Placeholder LP TOKEN: 0.30% Placeholder CP3R REWARDS: -%	0.000	Approve Deposit	MAX
CP3R CP3R Buy CP3R	-	-	CP3R Emissions CP3R REWARDS: -%	0.000	Approve Deposit	MAX

CP3R CP3R Buy CP3R	-	-	-%	CP3R Emissions CP3R REWARDS: -%	0.000	0.00000	MAX	Approve Deposit	Loading...	Claim
WBTC WBTC	-	-	-%	Placeholder Compound: -% Placeholder CP3R REWARDS: -%	0.000	0.00000	MAX	Approve Deposit	Loading...	Claim
Ethereum WETH	-	-	-%	Placeholder CP3R REWARDS: -%	0.000	0.00000	MAX	Approve Deposit	Loading...	Claim
DAI DAI	-	-	-%	Placeholder CURVE: -% Placeholder CP3R REWARDS: -%	0.000	0.00000	MAX	Approve Deposit	Loading...	Claim
Tether USDT	-	-	-%	Placeholder COMPOUND: -% Placeholder CP3R REWARDS: -%	0.000	0.00000	MAX	Approve Deposit	Loading...	Claim
USDC USDC	-	-	-%	Placeholder COMPOUND: -% Placeholder CP3R REWARDS: -%	0.000	0.00000	MAX	Approve Deposit	Loading...	Claim
YFI YFI	-	-	-%	Placeholder YFI Governance: -% Placeholder CP3R REWARDS: -%	0.000	0.00000	MAX	Approve Deposit	Loading...	Claim
UNI UNI	-	-	-%	Placeholder Compound: -% Placeholder CP3R REWARDS: -%	0.000	0.00000	MAX	Approve Deposit	Loading...	Claim
Placeholder COMPOUNDER.FINANCE										

<https://web.archive.org/web/20201124115606/https://etherscan.io/address/0x7ef1081ecc8b5b5130656a41d4c4f89dbcc8c>

The Compound.Finance contract was deployed by Ethereum address
0x079667f4f7a0B440Ad35ebd780eFd216751f0758 on 11/08/2020 01:50 UTC.

ETH Price: \$2,291.24 (-1.99%) Gas: 7.734 Gwei

Search by Address / Txn Hash / Block / Token / Domain Name

Home Blockchain Tokens NFTs Resources Developers More | Sign In

Etherscan

Transaction Details < >

Buy

Exchange

Play

Gaming

Sponsored: MetaWin: Compete for your share of \$1 MILLION in prizes. \$350k for 1st Place. Play Now!

Overview

Logs (1)

State

Transaction Hash:

0x170fe3b1aa976a30dd14f5f9a41b15113d9cab4c6b3c00aff705332cd661f1d8

Status:

Success

Block:

11213887 9514216 Block Confirmations

Timestamp:

1403 days ago (Nov-08-2020 01:50:47 AM UTC)

Transaction Action:

Call 0x60806040 Method by Compounder.Finance...

Sponsored:

From:

0x079667f4f7a0B440Ad35ebd780eFd216751f0758 (Compounder.Finance: Deployer)

To:

[0x7ef1081ecc8b5b5130656a41d4c4f89dbcc8c Created] (Compounder.Finance: CP3R Token)

Value:

0 ETH (\$0.00)

Transaction Fee:

0.04018816 ETH \$92.06

Gas Price:

20 Gwei (0.00000002 ETH)

Ether Price:

\$454.74 / ETH

Gas Limit & Usage by Txn:

8,000,000 | 2,009,408 (25.12%)

Other Attributes:

Nonce: 4 Position in Block: 19

Input Data:

0x60806040523480156200001157600000fd5b5060408051002018252600081526821a819a92a37b5b3b760b01b60208083019182528351808501909452600484526321a819a900e11b9084015281519192916200005f91600391620000f1565b508051620000759060049002084019062000f1565b50506005805460ff1916601217905550600062000091620000ed565b60058054610100600160a81b0319166101006001600160a01b03841690810291909117909155604051919250906000907f0be079c531659141344cd1fd0a4f28419497f9722a3daafe3b4186f6b6457e0908290a3506200018d56

View Input As Advanced Filter

More Details:

Click to show less

Private Note:

This website uses cookies to improve your experience. By continuing to use this website, you agree to its Terms and Privacy Policy.

Got It!

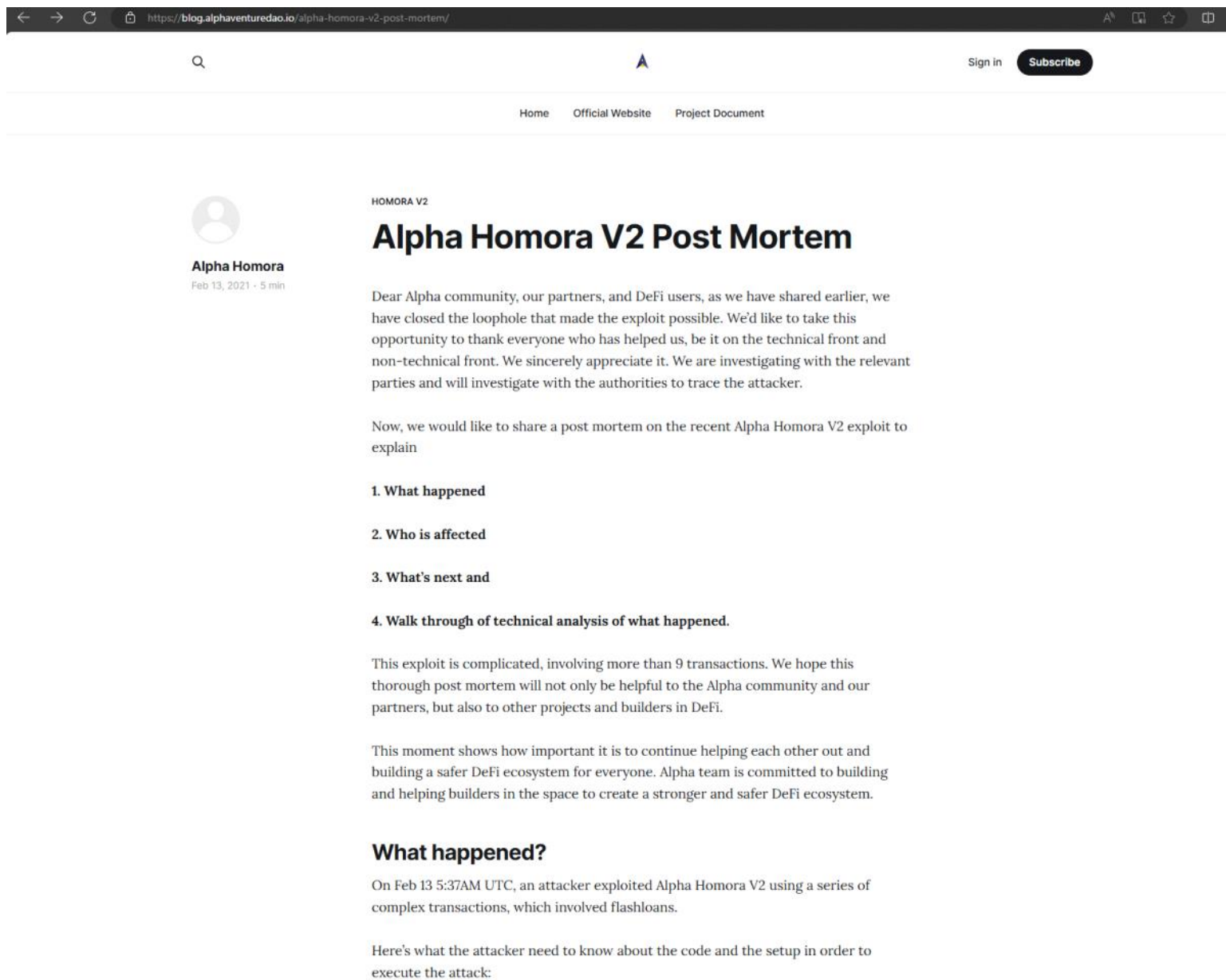
A transaction is a cryptographically signed instruction that changes the blockchain state. Block explorers track the details of all transactions in the network. Learn more about transactions in our Knowledge Base.

Tornado Cash Page 32

Alpha Homora

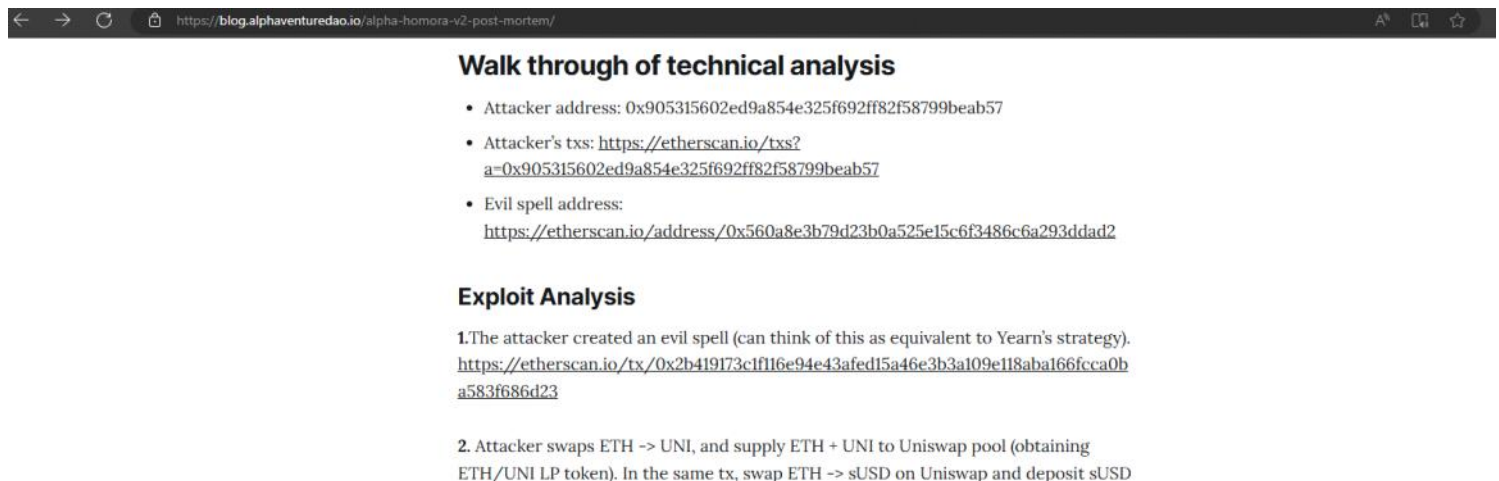
Wednesday, September 11, 2024 11:45 AM

On 02/13/2021 05:37 UTC, Alpha Homora DAO was hacked. Later that day, Alpha Homora released a post-mortem on their official website:



The screenshot shows a web browser displaying the Alpha Homora V2 Post Mortem blog post. The browser's address bar shows the URL: <https://blog.alphaventuredao.io/alpha-homora-v2-post-mortem/>. The website has a dark header with a search icon, a logo, and links for 'Sign in' and 'Subscribe'. Below the header, there are navigation links: 'Home', 'Official Website', and 'Project Document'. The main content area features a profile picture of Alpha Homora, the title 'Alpha Homora V2 Post Mortem', and a date 'Feb 13, 2021 · 5 min'. The text of the post begins with 'Dear Alpha community, our partners, and DeFi users, as we have shared earlier, we have closed the loophole that made the exploit possible. We'd like to take this opportunity to thank everyone who has helped us, be it on the technical front and non-technical front. We sincerely appreciate it. We are investigating with the relevant parties and will investigate with the authorities to trace the attacker.' It then states, 'Now, we would like to share a post mortem on the recent Alpha Homora V2 exploit to explain'. The post is structured with numbered sections: '1. What happened', '2. Who is affected', '3. What's next and', and '4. Walk through of technical analysis of what happened.' The text continues, 'This exploit is complicated, involving more than 9 transactions. We hope this thorough post mortem will not only be helpful to the Alpha community and our partners, but also to other projects and builders in DeFi.' It then says, 'This moment shows how important it is to continue helping each other out and building a safer DeFi ecosystem for everyone. Alpha team is committed to building and helping builders in the space to create a stronger and safer DeFi ecosystem.' The section 'What happened?' follows, stating, 'On Feb 13 5:37AM UTC, an attacker exploited Alpha Homora V2 using a series of complex transactions, which involved flashloans.' It concludes with, 'Here's what the attacker need to know about the code and the setup in order to execute the attack:'.

This blog post lays out a walkthrough and technical analysis of the exploit:



The screenshot shows the 'Walk through of technical analysis' section of the blog post. It lists three bullet points:

- Attacker address: 0x905315602ed9a854e325f692ff82f58799beab57
- Attacker's txs: <https://etherscan.io/txs?a=0x905315602ed9a854e325f692ff82f58799beab57>
- Evil spell address: <https://etherscan.io/address/0x560a8e3b79d23b0a525e15c6f3486c6a293ddad2>

 The section 'Exploit Analysis' follows, with two numbered points:

- The attacker created an evil spell (can think of this as equivalent to Yearn's strategy). <https://etherscan.io/tx/0x2b419173c1f116e94e43afed15a46e3b3a109e118aba166fcc0ba583f686d23>
- Attacker swaps ETH -> UNI, and supply ETH + UNI to Uniswap pool (obtaining ETH/UNI LP token). In the same tx, swap ETH -> sUSD on Uniswap and deposit sUSD

https://blog.alphaventuredao.io/alpha-homora-v2-post-mortem/

Walk through of technical analysis

- Attacker address: 0x905315602ed9a854e325f692ff82f58799beab57
- Attacker's txs: [https://etherscan.io/txs?
a=0x905315602ed9a854e325f692ff82f58799beab57](https://etherscan.io/txs?a=0x905315602ed9a854e325f692ff82f58799beab57)
- Evil spell address:
<https://etherscan.io/address/0x560a8e3b79d23b0a525e15c6f3486c6a293ddad2>

Exploit Analysis

1. The attacker created an evil spell (can think of this as equivalent to Yearn's strategy).
<https://etherscan.io/tx/0x2b419173c1f116e94e43afed15a46e3b3a109e118aba166fcca0ba583f686d23>

2. Attacker swaps ETH -> UNI, and supply ETH + UNI to Uniswap pool (obtaining ETH/UNI LP token). In the same tx, swap ETH -> sUSD on Uniswap and deposit sUSD to Cream's Iron Bank (getting cysUSD)
<https://etherscan.io/tx/0x4441eefe434fbef9d9b3acb169e35eb7b3958763b74c5617b390344dec4dd3ad>

3. Call execute to HomoraBankV2 using the evil spell (creating position 883), performing:

- Borrow 1000e18 sUSD
- Deposit UNI-WETH LP to WERC20, and use as collateral (to bypass the collateral > borrow check)
- In the process, the attacker has 1000e18 sUSD debt shares (because the attacker is the first borrower)

<https://etherscan.io/tx/0xcc57ac77dc3953de7832162ea4cd925970e064ead3f6861ee40076aca8e7e571>

4. Call execute to HomoraBankV2 using the evil spell again (to position 883), performing:

- Repay 1000000098548938710983 sUSD (actual debt with interest accrued is 10000000098548938710984 sUSD), resulting in a repay share of 1 less than the total share.
- As a result, the attacker now has 1 minisUSD debt and 1 debt share.

<https://etherscan.io/tx/0xf31ee9d9e83db3592601b854fe4f8b872cecd0ea2a3247c475e6a8062a20dd41>

The blog post also names the attacker's address as 0x905315602ed9a854e325f692ff82f58799beab57. The malicious contract was 0x560A8E3B79d23b0A525E15C6F3486c6A293DDAd2.

Below are the ERC20 transactions associated with this contract:

ETH Price: \$2,322.33 (-0.12%) Gas: 3,931 Gwei

Search by Address / Txn Hash / Block / Token / Domain Name

Etherscan Home Blockchain Tokens NFTs Resources Developers More Sign In

Token Transfers (ERC-20)

For 0x560a8e3b79d23b0a525e15c6f3486c6a293ddad2

Sponsored: Maker is now Sky. Get rewarded for saving without giving up control.

ⓘ Transactions involving tokens marked as suspicious, unsafe, spam or brand infringement are currently hidden. To show them, go to Site Settings.

ⓘ Transactions with zero token value are currently hidden. To show them, please go to Site Settings.

A total of 139 txns found [Download Page Data](#) First < Page 2 of 2 > Last

Transaction Hash	Method	Block	Date Time (UTC)	From	To	Amount	Token
0x64de824a7a...	Execute	11846623	2021-02-13 6:09:16	Cream.Finance: cySUS...	0x560A8E3B...A293DDAd2	131,885.08558758	Yearn Synth ... (cySUSD)
0x64de824a7a...	Execute	11846623	2021-02-13 6:09:16	0x560A8E3B...A293DDAd2	Cream.Finance: cySUS...	1,321.409764412	Synth sUSD (sUSD)
0x64de824a7a...	Execute	11846623	2021-02-13 6:09:16	0x5f5cd910...Cd00457bb	0x560A8E3B...A293DDAd2	661.350732531	Synth sUSD (sUSD)
0x64de824a7a...	Execute	11846623	2021-02-13 6:09:16	0x5f5cd910...Cd00457bb	0x560A8E3B...A293DDAd2	330.675366265	Synth sUSD (sUSD)

Try Roll

Wednesday, September 11, 2024 12:19 PM

On March 14, 2021, Try Roll posted on their website a blog post titled "Security Incident" that stated unknown attacker was able to gain access to the private keys of Tryroll's hot wallet. The stated that the malicious contract was 0xeaa86ddd49d8907c939413e92888536e4587bd9a and the malicious contract creator was 0x5fe4e7124d1da9046edc67a6499b565241be0167.

https://blog.tryroll.com/p/security-incident

Roll's Substack

Security Incident

ROLL TEAM
MAR 14, 2021

Share

Around 3:30am EST today, there was a security incident with Roll's hot wallet. As a result, the attacker was able to steal all the tokens from this wallet and sell on Uniswap for ETH. As of this writing, it seems like a compromise of the private keys of our hot wallet and not a bug in the Roll smart contracts or any token contracts. We are investigating this with our infrastructure provider and law enforcement.

Attacker contract:
<https://etherscan.io/address/0xeaa86ddd49d8907c939413e92888536e4587bd9a>

Attacker contract creator:
<https://etherscan.io/address/0x5fe4e7124d1da9046edc67a6499b565241be0167>

Thank you to everyone that reached out to find ways to support. The attacker has already sold all the tokens. There is no further user action suggested at this stage. We are temporarily disabling withdraw from the Roll wallet of all social money until we have migrated our hot wallet.

It is hard to put into words how devastating this is and we are really sorry about what happened. We take security very seriously and strive to earn the trust of our creators and communities with their social money but today we messed up.

We will do a third-party audit of our security infrastructure over the coming days to ensure this never happens again. We will also run a forensic analysis to figure out how the key was compromised.

In the meantime, we are announcing a \$500,000 fund to help the creators and their communities affected by this. We will reach out to every community one by one in coming days and will give more details soon.

An analysis of the malicious contract, shows the ERC20 tokens transferred from the hot wallet and swapped for Ether:

Etherscan

Home

Blockchain

Tokens

NFTs

Resources

Developers

More

Sign In

Token Transfers (ERC-20)

For 0xeaa86ddd49d8907c939413e92888536e4587bd9a

Sponsored: MetaWin: Compete for your share of \$ 1 MILLION in prizes. \$350k for 1st Place. Play Now!

A total of 84 txns found

Download Page Data

First

<

Page 1 of 2

>

Last

Transaction Hash	Method	Block	Age	From	To	Amount	Token
<div>0xfa36e3169be...</div>	<div>0x51c3b99f</div>	<div>12035408</div>	<div>1277 days ago</div>	<div>0xeaa86ddd...E4587Bd9A</div>	<div>OUT</div> <div>Uniswap V2: WHALE</div>	<div>217,000.52</div>	<div>WHALE (WHALE)</div>
<div>0xfa36e3169be...</div>	<div>0x51c3b99f</div>	<div>12035408</div>	<div>1277 days ago</div>	<div>0xeaa86ddd...E4587Bd9A</div>	<div>OUT</div> <div>Uniswap V2: FWB</div>	<div>2,616,526.32</div>	<div>FRIENDS WITH... (FWB)</div>
<div>0xfa36e3169be...</div>	<div>0x51c3b99f</div>	<div>12035408</div>	<div>1277 days ago</div>	<div>0xeaa86ddd...E4587Bd9A</div>	<div>OUT</div> <div>Uniswap V2: KARMA</div>	<div>3,203,291</div>	<div>Karma (KARMA)</div>
<div>0xfa36e3169be...</div>	<div>0x51c3b99f</div>	<div>12035408</div>	<div>1277 days ago</div>	<div>0xeaa86ddd...E4587Bd9A</div>	<div>OUT</div> <div>Uniswap V2: JULIEN</div>	<div>287,103</div>	<div>Julien (JULIEN)</div>
<div>0xfa36e3169be...</div>	<div>0x51c3b99f</div>	<div>12035408</div>	<div>1277 days ago</div>	<div>0xeaa86ddd...E4587Bd9A</div>	<div>OUT</div> <div>Uniswap V2: 1337 2</div>	<div>400,001</div>	<div>1337 (1337)</div>

Bitmart


Wednesday, September 11, 2024 1:08 PM

On December 7, 2021, exchange Bitmart announced on their official blog that there was a security incident where an actor stole private keys for their BSC and ETH hot wallets. The incident happened on December 4, 2021 and resulted in an approximate loss of \$200 million.


← ↻ 🔒 <https://bitmart-exchange.medium.com/bitmart-response-to-security-breach-71ccc2200285>

Medium 🔍 Search

BitMart Response to Security Breach

 BitMart Exchange · Follow
1 min read · Dec 7, 2021

🕒 4 💬 1 🌟 🔄 📄



On December 4, 2021, at approximately 6:30 pm EST, BitMart identified a security breach related to two of its hot wallets. Within moments, a security response was activated, with multiple systems shut down procedurally to prevent additional losses, including account withdrawals and the trading of certain pairs.

In concert with leading firms worldwide, a comprehensive security review and investigation was enacted and remains ongoing. Findings thus far indicate that the breach affected two hot wallets: one BSC wallet and one ETH wallet. Based on initial investigation, it appears that approximately \$200 million in digital assets were removed by a malicious actor who had gained access to critical private keys.

Since the breach, BitMart has begun extraordinary efforts to ensure the lasting security of its customers and their funds.

Bitmart's CEO Sheldon Xia also release a series of tweets describing the incident:

🔒 <https://x.com/sheldonbitmart>

 Settings

← **Sheldon**  419 posts Follow

🗨️ 3.3K 🔄 1.6K ❤️ 1.2K 📊 📄 📤

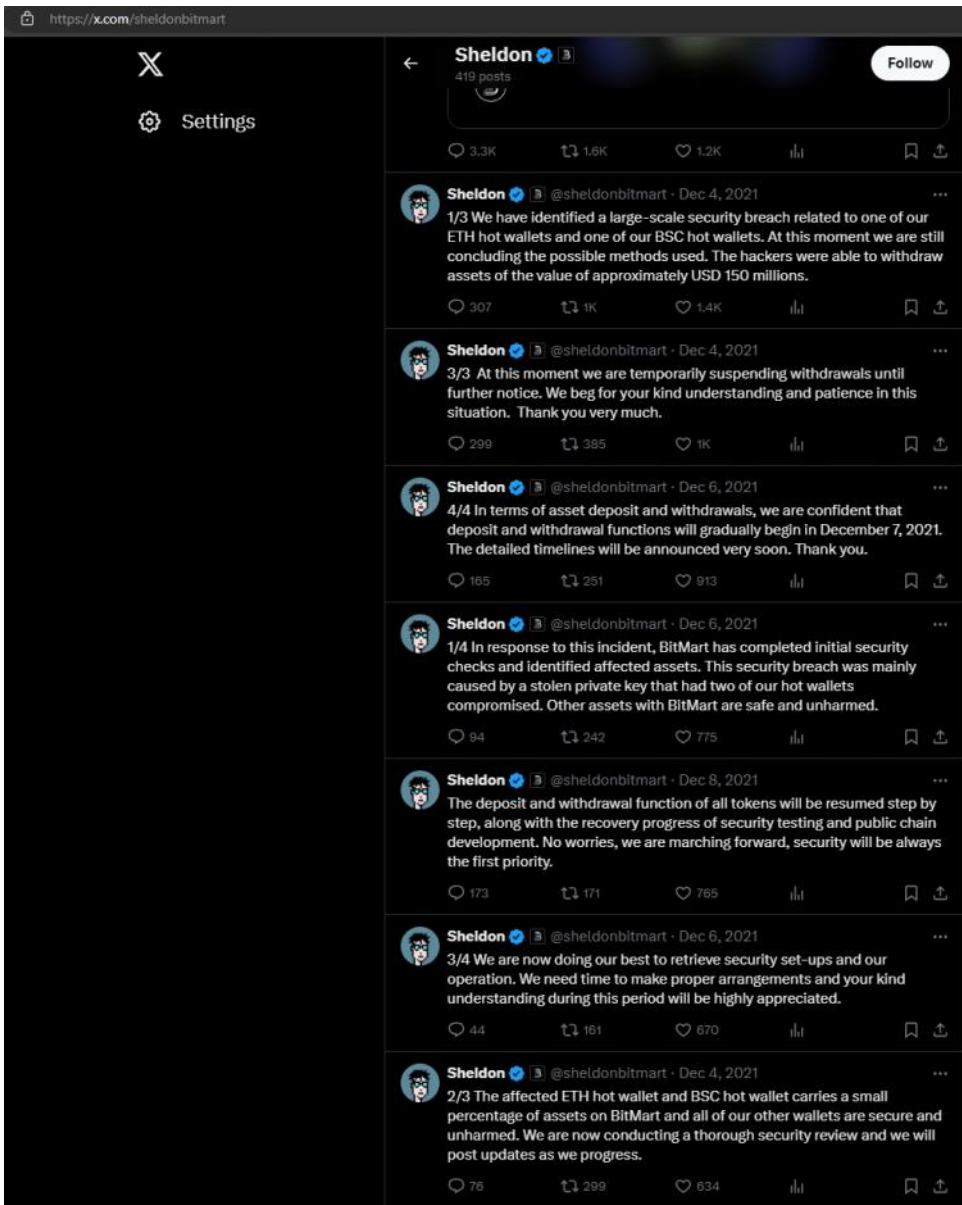
 **Sheldon**  @sheldonbitmart · Dec 4, 2021

1/3 We have identified a large-scale security breach related to one of our ETH hot wallets and one of our BSC hot wallets. At this moment we are still concluding the possible methods used. The hackers were able to withdraw assets of the value of approximately USD 150 millions.

🗨️ 307 🔄 1K ❤️ 1.4K 📊 📄 📤

 **Sheldon**  @sheldonbitmart · Dec 4, 2021

3/3 At this moment we are temporarily suspending withdrawals until further notice. We beg for your kind understanding and patience in this situation. Thank you very much.



An analysis of Bitmart's ETH and BSC hot wallets on 12/04/2021 shows large outflows of ERC20 tokens to Ethereum attacker wallet 0x39f80dcd139458835d47410Ae0DE7181D3edf270 and Binance Smart Chain attacker wallet 0x25fb126b6c6b5c8ef732b86822fa0f0024e16c61.

Here are BSC token transfers showing the Bitmart hacker stealing tokens from the Bitmart BSC smart chain:

https://bscscan.com/tokentransfers?a=0x25fb126b6c6b5c8ef732b86822fa0f0024e16c61&ps=100&p=2									
BNB Price: \$533.03 (+2.82%) Gas: 1 GWei		Search by Address / Txn Hash / Block / Token / Domain Name							
Transaction Hash	Method	Block	Date (UTC)	From	To	Amount	Token		
0x8818ff62ac8...	Swap	13200067	2021-12-04 23:11:36	Bitmart Hacker	OUT 0x3790C9B5...c9B868E1e	352,346.046550693	Binance-Peg ... (BSC-USD)		
0x9a0726bd2d...	Swap	13199987	2021-12-04 23:07:35	Bitmart Hacker	OUT 0x3790C9B5...c9B868E1e	17,517,574,883,796.872694994	SafeMoon (SAFEMOON)		
0x9a8cce677f9...	Swap	13199946	2021-12-04 23:05:32	Bitmart Hacker	OUT 0x3790C9B5...c9B868E1e	15,407,093,855.144345483	FLOKI (FLOKI)		
0x90a4358e2f3...	Swap	13199890	2021-12-04 23:02:44	Bitmart Hacker	OUT 0x3790C9B5...c9B868E1e	9,000,000,000,000	SafeMoon (SAFEMOON)		
0xeb1ec1436d...	Transfer	13199328	2021-12-04 22:34:38	Bitmart 12	IN Bitmart Hacker	352,346.046550693	Binance-Peg ... (BSC-USD)		
0x6709cf1e25e...	Transfer	13199075	2021-12-04 22:21:59	Bitmart 12	IN Bitmart Hacker	75,603,865,478,198.39864008	Safe Energy (EnergyX)		
0x0e61808367...	Transfer	13199072	2021-12-04 22:21:50	Bitmart 12	IN Bitmart Hacker	2,332,295.789080055	StackOS (STACK)		
0xbc35b601d2...	Transfer	13199068	2021-12-04 22:21:38	Bitmart 12	IN Bitmart Hacker	92,740,731.479772929	BNBPay (BPAY)		
0xc44efec4e6d...	Transfer	13199064	2021-12-04 22:21:26	Bitmart 12	IN Bitmart Hacker	110,372,682,133,179.940163682	Moonshot (MOONSHOT)		
0x91c6ae6e10...	Transfer	13199060	2021-12-04 22:21:14	Bitmart 12	IN Bitmart Hacker	3,806,819.72915495	ZOE CASH (ZOE)		

Beanstalk

Wednesday, September 11, 2024 4:23 PM

04/19/2022, Beanstalk released a statement on their official blog explaining that on 04/17/2022 at approximately 12:24 UTC approximately \$77 million was stolen using an exploit in the Beanstalk protocol.

<https://bean.money/blog/beanstalk-governance-exploit>



Blog

Beanstalk Farms · April 19th, 2022

Beanstalk Governance Exploit

Beanstalk was attacked on April 17, resulting in a theft of ~\$77M in non-Beanstalk user assets.

- [Technical Breakdown](#)
- [Path Forward](#)
- [A Farmer's Guide to the Barn Raise](#)
- [Anticipated Replant Timeline](#)

Beanstalk, a decentralized credit based stablecoin protocol, was attacked at roughly 12:24pm UTC on April 17, resulting in a theft of ~\$77M in non-Beanstalk user assets. The perpetrator used a flash loan to exploit the protocol's governance mechanism and send the funds to a wallet they controlled. Beanstalk Farms, the decentralized development team working on Beanstalk, is preparing a strategy to safely re-launch a more secure Beanstalk with a path forward.

Yesterday morning, the Beanstalk contract on the Ethereum mainnet was exploited via a previously-unknown issue with Beanstalk's governance process. The Beanstalk Farms team was immediately alerted and took action to temporarily shut off protocol governance and pause Beanstalk. Approximately \$77M was stolen from the protocol's liquidity pools. The team has since burned the remaining Beans in the exploiter contract.

Since the attack, the Beanstalk community has demonstrated incredible support for the project and provided numerous thoughtful ideas for a suitable path forward. The Beanstalk Farms team has taken these ideas into consideration and developed a proposal with four primary goals in mind: securing the enduring success of Beanstalk's economic model; attracting sufficient capital to restart Beanstalk; preserving as much of each Farmers' Stalk, Seed and Pod positions as possible, and; aligning new capital with previous Stalk and Pod holders.

About Beanstalk

Beanstalk is a decentralized protocol that allows anyone to realize the value of an open, credit based stablecoin. The Beanstalk community of lenders, borrowers and savers secures a protocol-native stablecoin, Bean, with the goal of creating the world's most accessible digital money system. By eliminating collateral requirements, Beanstalk aims to be the catalyst for a trustless solution to unlock the universal potential of decentralized finance.

The "Technical Breakdown" link leads to a blog post on Medium.com titled "Beanstalk \$BEAN Exploit". In this article, specific technical details about the exploit are explained. This article states that the attacker's Ethereum address was 0x1c5dcd006ea78a7e4783f9e6021c32935a10fb4.

Secondly, approximately nine minutes later, the same address deposited the 212,858 BEAN into the Beanstalk Silo

(<https://etherscan.io/tx/0xf5a698984485d01e09744e8d7b8ca15cd29aa430a0137349c8c9e19e60c0bb9d>)

Thirdly, since a proportionate amount of *Stalk* is immediately generated upon a whitelisted asset deposit, this Silo deposit allowed the address to propose Beanstalk Improvement Proposals (BIP) 18

(<https://etherscan.io/tx/0x68cdec0ac76454c3b0f7af0b8a3895db00adf6daaf3b50a99716858c4fa54c6f/advanced>) and 19

(<https://etherscan.io/tx/0x9575e478d7c542558ecca52b27072fa1f1ec70679106bdbd62f3bb4d6c87a80d>).

BIP-18 was originally left blank, and BIP-19 (exploiter named it InitBip18, we'll get to that later) contained a verified contract that proposed a \$250k donation to the Ukraine wallet address, as well as \$10k to the proposer.

```

1 // SPDX-License-Identifier: MIT
2 pragma solidity 0.8.13;
3
4 // Ukraine Donation Proposal
5 // Give 250,000 Bean to Ukraine (and 10,000 Bean to the proposer)
6
7 * abstract contract IBean {
8     function mint(address account, uint256 amount) public virtual returns (bool);
9 }
10
11 * contract InitBip18 {
12     address private constant bean = 0xDC59ac4FeFa32293A958890c396682858d52e50b; // Bean Address
13     address private constant proposerWallet = 0xE5eCF73603D98A0128F05ed30506ac7A663d8b69; // Proposer Wallet
14     address private constant ukraineWallet = 0x165CD37b4C644C2921454429E7F9358d18A45e14; // Ukraine Wallet
15     uint256 private constant proposerAmount = 10_000 * 1e6; // 10,000 Beans
16     uint256 private constant donationAmount = 250_000 * 1e6; // 250,000 Beans
17
18     function init() external {
19         IBean(bean).mint(proposerWallet, proposerAmount);
20         IBean(bean).mint(ukraineWallet, donationAmount);
21     }
22 }

```

Source: <https://etherscan.io/address/0x259a2795624b8a17bc7eb312a94504ad0f615d1e#code>

An analysis of this address shows the attacker stealing approximately 24,830 ETH as described in the technical breakdown:

Furucombo

Wednesday, September 11, 2024 4:59 PM

On 02/27/2021, DeFi platform Furucombo was exploited and approximately \$15 million was stolen. Furucombo announced this exploit on their official blog:

<https://medium.com/furucombo/furucombo-post-mortem-march-2021-ad19afd415e>

um Search

✦ Get unlimited access to the best of Medium for less than \$1/week. [Become a member](#)

Furucombo Post-Mortem March 2021



FURUCOMBO · Follow

Published in FURUCOMBO · 4 min read · Mar 1, 2021

👍 323



Update

To add an extra layer of protection to Furucombo, we've made the following updates:

1. Frontend Feature: Only approve the amount spent.
2. Redeploy Proxy: Make sure the token allowances of users are 0.
- The new proxy contract address:

0xA013AfbB9A92cEF49e898C87C060e6660E050569

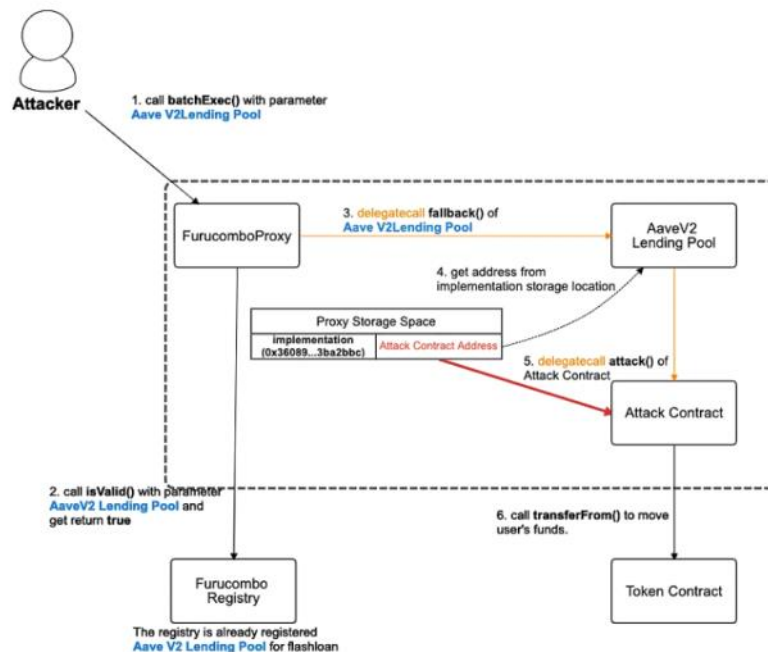
*Aave cubes and flashloan are temporarily down as we are undergoing thorough testing.

Original Post

Dear Furucombo community, DeFi users, and partners, we'd like to share a full update on the recent exploit that took place.

In this post, we will outline what happened during the exploit that occurred on Saturday 27 February 2021, explain who was affected, outline what we are doing and provide the next steps of how we will prevent this from occurring again.

The technical section of this blog post revealed a transaction associated with the hacker:
0xfaf46447572617a7eef027be43525b3168e4b650c07a50338faa453dda1f1940



After the compromise was discovered, we immediately removed the Aave v2 lending pool from the registry contract at 05:46:16 PM UTC, as this was the key element of the attack. The attacker's transaction at 05:55:17 PM UTC was then reverted [4]. Though the handler was not affected, we temporarily paused the function of Aave cubes. The rest of the cubes remain functional.

...

Links

- Website: furucombo.app
- Discord: discord.furucombo.app
- Forum: forum.furucombo.app

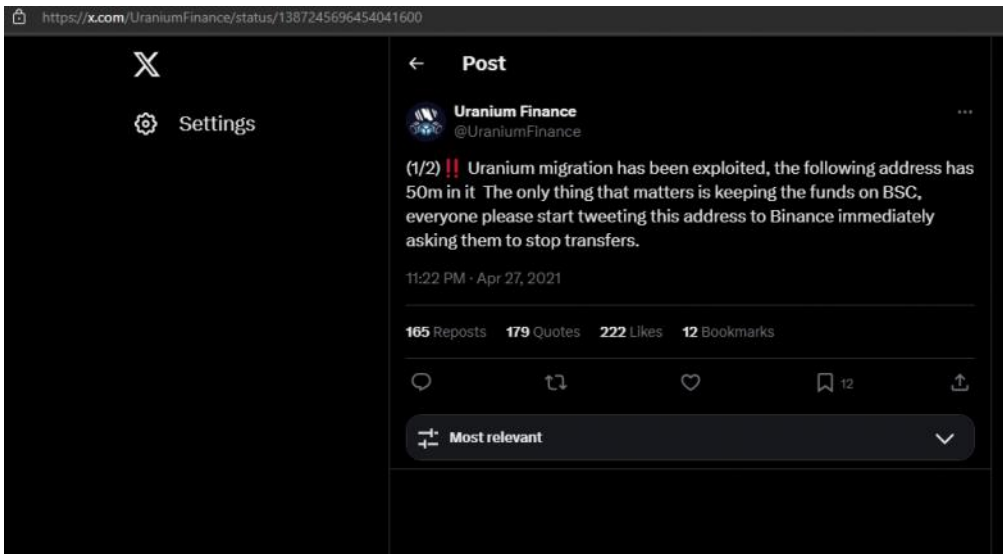
<https://etherscan.io/tx/0xfaf46447572617a7eef027be43525b3168e4b650c07e50338faa453dda1f1940> team@furucombo.app

An analysis of this transaction shows that the hacker's wallet is:
0xb624E2b10b84a41687caeC948Dd484E48d76B212

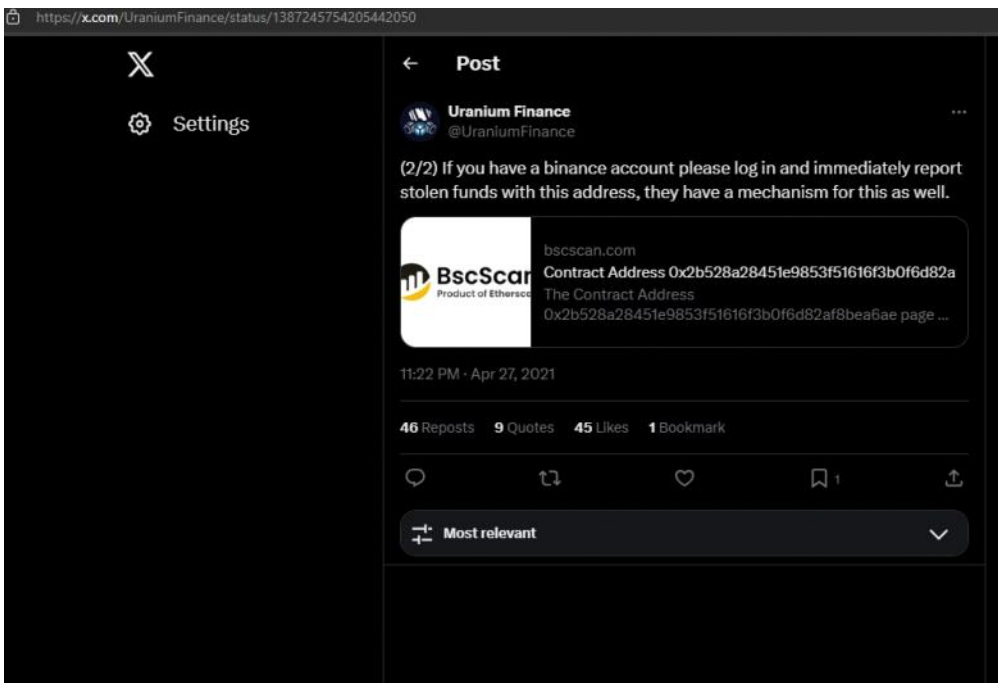
Uranium Finance

Wednesday, September 11, 2024 5:54 PM

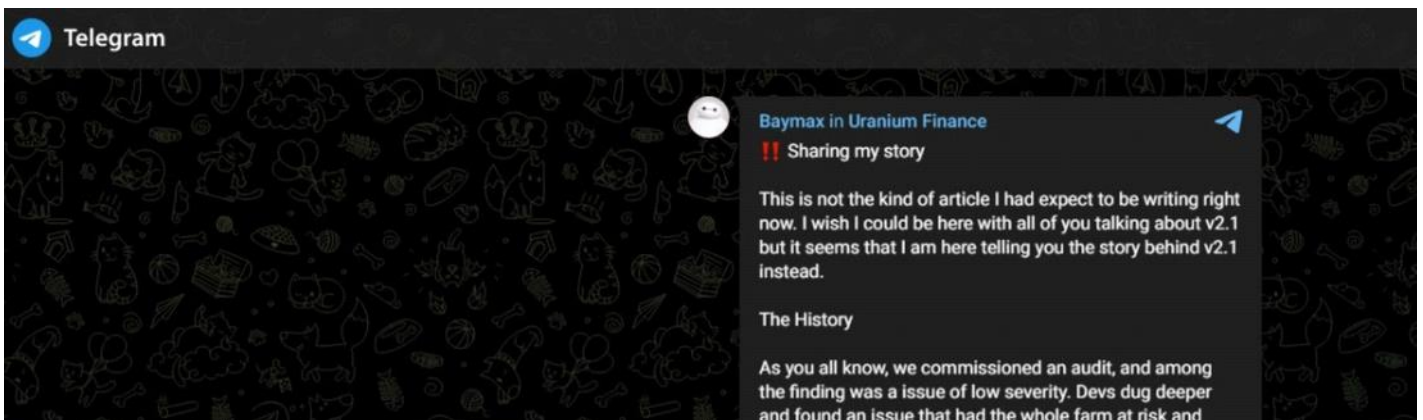
On 04/27/2021 the official Uranium Finance Twitter account tweeted that their protocol had been exploited:

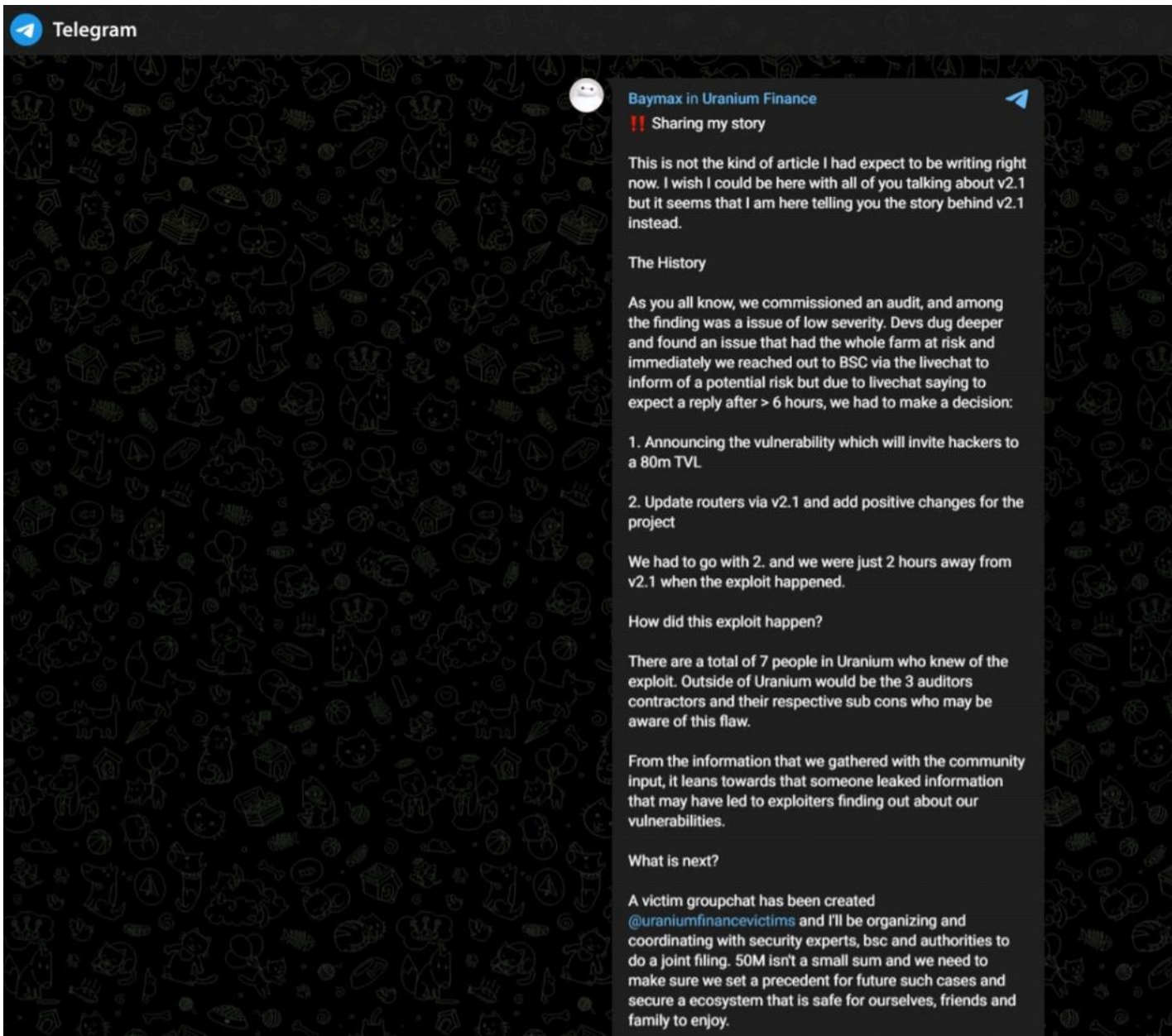


They sent a second tweet stating the contract address of the hacker:



On 04/28/2021, in a post to their Telegram channel, Uranium Finance described how the exploit worked:





An analysis of the malicious contract shows that its creator was 0xC47BdD0A852a88A019385ea3f57Cf8de79F019d:

https://bscscan.com/tx/0xdfae4d0ce12bc88ea4189633dbec9c0e3d788e09fe86ecc9427cddd7e2cb3

BNB Price: \$529.67 (+1.74%) Gas: 1 GWei

Search by Address / Txn Hash / Block / Token / Domain Name

BscScan
Product of Etherscan

Home Blockchain Validators Tokens NFTs Resources Developers More

Transaction Details < > Buy

Sponsored: Rollbit: The largest Solana Gaming Platform. Over 11,000,000 SOL won. Instant withdrawals! [Play Now!](#)

Overview State

Transaction Hash: 0xdfae4d0ce12bc88ea4189633dbec9c0e3d788e09fe86ecc9427cddd7e2cb3

Status: Success

Block: 6946649 35225301 Block Confirmations

Timestamp: 1232 days ago (Apr-28-2021 02:37:37 AM UTC)

Transaction Action: Call 0x60806040 Method by 0xC47BdD0A...de79F019d

Sponsored:

Transaction Action: [Call](#) [0x60806040](#) Method by [0xC47BdD0A...de79F019d](#)

Sponsored:

From: [0xC47BdD0A852a88A019385ea3ff57cf8de79F019d](#)

To: [\[0x2b528a28451e9853f51616f3b0f6d82af8bea6ae Created \]](#)

Value: 0 BNB (\$0.00)

Transaction Fee: 0.00387495 BNB **\$2.05**

Gas Price: 5 Gwei (0.000000005 BNB)

More Details: [+ Click to show more](#)

Private Note: To access the Private Note feature, you must be [Logged In](#)

⚡ A transaction is a cryptographically signed instruction that changes the blockchain state. Block explorers track the details of all transactions in the network. Learn more about transactions in our Knowledge Base.

An analysis of the token transactions in this account shows the tokens being stolen on 04/28/2021:

https://bscscan.com/tokens?address=0xc47bdd0a852a88a019385ea3ff57cf8de79f019d&ps=100

BNB Price: \$529.26 (+1.66%) Gas: 1 Gwei

Search by Address / Txn Hash / Block / Token / Domain Name

Address	Operation	Block	Time	From	Direction	To	Value	Token
0xd9b484b592...	Swap	6948503	2021-04-28 4:10:19	0xC47BdD0A...de79F019d	OUT	0x146CD24d...D25aFA9C0	632.6222	Binance-Peg ... (ET)
0x41390d366d...	Swapout	6948480	2021-04-28 4:09:10	0xC47BdD0A...de79F019d	OUT	Null: 0x000...000	200	ANY Ethereum (any)
0xf2c6dbd0a9...	Swap Exact T...	6948461	2021-04-28 4:08:13	0x74E4716E...9F18a4fbc	IN	0xC47BdD0A...de79F019d	303.45462858	Binance-Peg ... (ET)
0xf2c6dbd0a9...	Swap Exact T...	6948461	2021-04-28 4:08:13	0xC47BdD0A...de79F019d	OUT	0x28415ff2...5ab9d031F	638,071.293091598	Binance-Peg ... (AD)
0x257fba9b7f6...	Swap Exact T...	6948444	2021-04-28 4:07:22	0x74E4716E...9F18a4fbc	IN	0xC47BdD0A...de79F019d	329.167542169	Binance-Peg ... (ET)
0x257fba9b7f6...	Swap Exact T...	6948444	2021-04-28 4:07:22	0xC47BdD0A...de79F019d	OUT	0xDd5bAd8f...2fe0022CF	26,520.084603305	Binance-Peg ... (DC)
0xfb3d534f269...	Swapout	6948398	2021-04-28 4:05:04	0xC47BdD0A...de79F019d	OUT	Null: 0x000...000	200	ANY Ethereum (any)
0xddce028004...	Transfer From	6948388	2021-04-28 4:04:34	0x2b528a28...Af8bEA6Ae	IN	0xC47BdD0A...de79F019d	638,071.193091598	Binance-Peg ... (AD)
0x922a1abde1...	Transfer From	6948356	2021-04-28 4:02:58	0x2b528a28...Af8bEA6Ae	IN	0xC47BdD0A...de79F019d	26,519.084603305	Binance-Peg ... (DC)
0x4d7e172e6b...	Swapout	6948266	2021-04-28 3:58:28	0xC47BdD0A...de79F019d	OUT	Null: 0x000...000	200	ANY Ethereum (any)
0xbcc63389fe7b...	Swapout	6948248	2021-04-28 3:57:34	0xC47BdD0A...de79F019d	OUT	Null: 0x000...000	80.09349843	ANY Bitcoin (anyB1)
0xd0c681a94b...	Swap	6948207	2021-04-28 3:55:31	0x6C341938...c66E6270c	IN	0xC47BdD0A...de79F019d	80.09349843	ANY Bitcoin (anyB1)
0xd0c681a94b...	Swap	6948207	2021-04-28 3:55:31	0xC47BdD0A...de79F019d	OUT	0x6C341938...c66E6270c	80.3128	Binance-Peg ... (BT)
0x054f92903ae...	Swapout	6948185	2021-04-28 3:54:25	0xC47BdD0A...de79F019d	OUT	Null: 0x000...000	200	ANY Ethereum (any)
0x4494ac3680...	Transfer From	6948177	2021-04-28 3:54:01	0x2b528a28...Af8bEA6Ae	IN	0xC47BdD0A...de79F019d	80.311826556	Binance-Peg ... (BT)
0x7a79e1220c...	Swapout	6948129	2021-04-28 3:51:37	0xC47BdD0A...de79F019d	OUT	Null: 0x000...000	200	ANY Ethereum (any)
0x8991f2c3885...	Swapout	6948044	2021-04-28 3:47:22	0xC47BdD0A...de79F019d	OUT	Null: 0x000...000	200	ANY Ethereum (any)
0x09fe6fe02f2...	Swapout	6947955	2021-04-28 3:42:55	0xC47BdD0A...de79F019d	OUT	Null: 0x000...000	200	ANY Ethereum (any)
0xbfeb95b1383...	Swapout	6947905	2021-04-28 3:40:25	0xC47BdD0A...de79F019d	OUT	Null: 0x000...000	200	ANY Ethereum (any)
0xfdd300ca829...	Swapout	6947791	2021-04-28 3:34:43	0xC47BdD0A...de79F019d	OUT	Null: 0x000...000	200	ANY Ethereum (any)
0x1c23ec4895...	Swap	6947764	2021-04-28 3:33:22	0x146CD24d...D25aFA9C0	IN	0xC47BdD0A...de79F019d	1,808.666977924	ANY Ethereum (any)
0x1c23ec4895...	Swap	6947764	2021-04-28 3:33:22	0xC47BdD0A...de79F019d	OUT	0x146CD24d...D25aFA9C0	1,813.1532	Binance-Peg ... (ET)
0xc286401d6b...	Send Token	6947725	2021-04-28 3:31:25	0x2b528a28...Af8bEA6Ae	IN	0xC47BdD0A...de79F019d	1,812.523766875	Binance-Peg ... (ET)

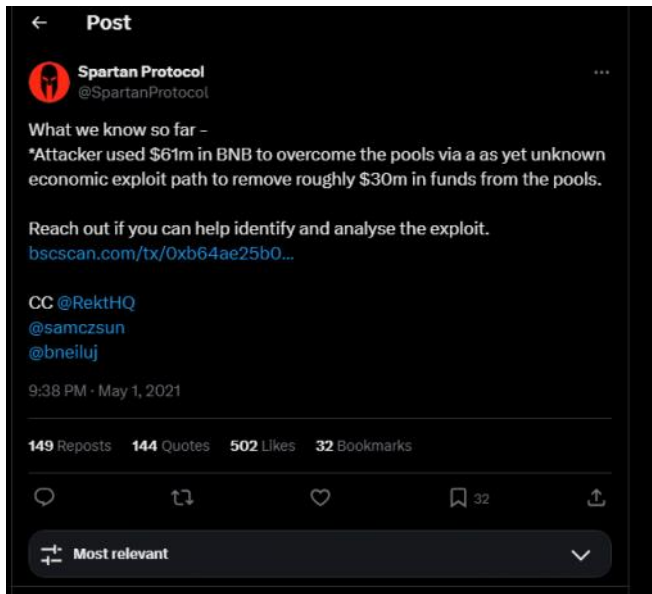
Shortly thereafter, the hacker swaps the stolen tokens for ETH sent to address [0xc61429117038A1f13881DD7410880771F28e06ec](#).

[0xfdd300ca82956b6440ce7f13c0aa0d4868a2772063ab5b58bd4e547853248bfd](#)

Spartan Protocol

Wednesday, September 11, 2024 6:36 PM

On 05/01/2021, the official Spartan Protocol Twitter account announced they had been hacked and the hackers BSC address was 0x3B6e77722e2bBe97C1cfA337B42C0939AEb83671.



An analysis of token transfers of this address show the hacker executing the heist:

PAID Network

Thursday, September 12, 2024 10:28 AM

On 3/7/2021, PAID Network published a postmortem on their Medium.com account stating that they were hacked on 03/05/2021 at 18:00 UTC. Specifically, the attacker used stolen private keys to steal approximately 59.48 million PAID tokens.

https://paidnetwork.medium.com/paid-network-attack-postmortem-march-7-2021-9e4c0fef0e07

PAID NETWORK · Follow
5 min read · Mar 6, 2021

1.4K 20

PAID Network Attack Postmortem, March 7, 2021

Letter From Kyle Chassé

Dear PAID community,

First of all I would like to thank everyone for their unwavering support while we investigated the attack that happened on Friday, March 5th, at 20:00 UTC+2. An attacker exploited the PAID Network deployer contract to steal over 59 million PAID tokens.

The attacker used a compromised private key to the original contract deployer to leverage the upgrade function of the smart contract. The attacker then proceeded to 'upgrade' to a new smart contract which had the ability to burn and re-mint tokens.

With the upgraded smart contract, the attacker then minted 59,471,745.571 PAID tokens which they then proceeded to sell. 2,501,203 \$PAID tokens on Uniswap were sold for a total of 2,040.4339 ETH before the attack was discovered at 20:17 UTC+2. Upon discovery the PAID team pulled liquidity from Uniswap, minimizing damage. We then asked all PAID token holders to cease all transactions in order to mitigate further risk. We called in industry experts (Cipherblade, Parsiq, Acheron, CertiK and Immunefi) to further safeguard users and specify next steps.

To prevent any further damage by the attacker, PAID Network is relaunching its token to wipe the attacker from the ledger of token holders, moving control of the new token contract to a multisig, and securing comprehensive security and process audits to ensure we are never again vulnerable to this kind of attack or others.

This blog further details in the "Technical Analysis of the Attack" section that the transaction hash of 0x4bb10927ea7afc2336033574b74ebd6f73ef35ac0db1bb96229627c9d77555a0 shows where the attacker sends the stolen PAID coin to his Ethereum address.

https://paidnetwork.medium.com/paid-network-attack-postmortem-march-7-2021-9e4c0fef0e07

believe the transfer was total and complete to the fullest extent. We were mistaken, and assume full responsibility for our lack of thorough verification.

As a result, the attacker proceeded to use the compromised private key to do the following:

1. Attacker loads contract deployer address with ETH. Tx:
<https://etherscan.io/tx/0x28494ebcd854735e4d84f55890f0a92376d1af17553d998b2ee391a25dbc18c7>
2. Attacker calls 'transferOwnership' function on PAID token contract from

https://paidnetwork.medium.com/paid-network-attack-postmortem-march-7-2021-9e4c0fef0e07

believe the transfer was total and complete to the fullest extent. We were mistaken, and assume full responsibility for our lack of thorough verification.

As a result, the attacker proceeded to use the compromised private key to do the following:

1. Attacker loads contract deployer address with ETH. Tx:
<https://etherscan.io/tx/0x28494ebcd854735e4d84f55890f0a92376d1af17553d998b2ee391a25dbc18c7>
2. Attacker calls 'transferOwnership' function on PAID token contract from PAID deployer address. Tx:
<https://etherscan.io/tx/0x733dd279b3d24f3415f3850b8eaceafc651c1998163dcd0352b9e83c46e2b33d9>
3. Attacker deploys a new contract. Tx:
<https://etherscan.io/tx/0xfe6eb5800741e986d6375d8e3f94eefd00cc64ba8896389142fdb6162a34d9b8>
4. Attackers burns PAID tokens on the staking rewards address. Tx:
<https://etherscan.io/tx/0x3a483dd881d98541ebbd51e9a64daa700546bae9c2b33a30c2192f9981334b9b>
5. Attacker mints 59,471,745.571 tokens, which he sends to his address. Tx:
<https://etherscan.io/tx/0x4bb10927ea7afc2336033574b74ebd6f73ef35ac0db1bb96229627c9d77555a0>
6. Attacker approves trading on Uniswap for his address. Tx:
<https://etherscan.io/tx/0x1a23506c2a53e9811ebe7ab9d78ba1ab9e02766d2440ff152437a3176a314a38>
7. Attacker proceeds to sell 2,501,203 \$PAID tokens on Uniswap for a total of 2,040.4339 ETH before being stopped by the PAID Network team's efforts to pull Uniswap liquidity. All funds (PAID and ETH) remain at the attacker's address, found here:
<https://etherscan.io/address/0x18738290af1aaf96f0acfa945c9c31ab21cd65be>

An analysis of that transaction shows that the attacker's address is 0x18738290AF1Aaf96f0AcFA945C9C31aB21cd65bE:

https://etherscan.io/tx/0x4bb10927ea7afc2336033574b74ebd6f73ef35ac0db1bb96229627c9d77555a0

ETH Price: \$2,356.96 (+2.06%) Gas: 7.501 Gwei

Search by Address / Txn Hash / Block / Token / Domain Name

Etherscan Home Blockchain Tokens NFTs Resources Developers More Sign In

Transaction Details

Sponsored: MetaWin: Compete for your share of \$1 MILLION in prizes. \$350k for 1st Place. Play Now!

Overview Internal Txns Logs (1) State

Transaction Hash: 0x4bb10927ea7afc2336033574b74ebd6f73ef35ac0db1bb96229627c9d77555a0

Status: Success

Block: 11979840 8755310 Block Confirmations

Timestamp: 1286 days ago (Mar-05-2021 06:03:09 PM UTC)

Transaction Action: Transfer 59,471,745.571 PAID To 0x18738290AF1Aaf96f0AcFA945C9C31aB21cd65bE

Sponsored:

From: 0x18738290AF1Aaf96f0AcFA945C9C31aB21cd65bE

Interacted With (To): 0x8c8687fc965593DFb2F0b4EAeFD55E9D8df348df (PAID Network: Old Contract)

Rari Capital 2021

Thursday, September 12, 2024 10:59 AM

On 05/08/2021, David Lucid, a cofounder of Rari Capital, published on Medium.com a post-mortem on an exploit of their protocol. In his blog, he states that the exploit took place in the morning of 05/08/2021 and resulted in the stealing of approximately 2,600 ETH.

Specifically, Lucid explains that the exploit involved Rari Capital's connection with Alpha Finance.

medium.com/rari-capital/5-8-2021-rari-ethereum-pool-post-mortem-60aab5af6f99

Search


Get unlimited access to the best of Medium for less than \$1/week. [Become a member](#)

5/8/2021: Rari Capital Ethereum Pool — Post-Mortem

Details on the Rari Capital Ethereum Pool hack on May 8, 2021

David Lucid · Follow
Published in Rari Capital · 3 min read · May 8, 2021

269 2



This morning, an attacker stole approximately 2600 ETH, around \$10m USD at the time of writing. These funds were extracted from Rari Capital's Ethereum Pool before the attacker was stopped when the contracts were paused. This loss equates to 60% of all users' funds in the Rari Capital Ethereum Pool.

As core contributors to the protocol, we take such an attack extremely seriously. Below, we describe in detail exactly what happened and the primary steps we will be taking to proactively prevent attacks from happening in the future. In the next couple days, you can expect another blog post describing the potential paths towards making everyone whole again.

The Rari Capital Ethereum Pool deposits ETH into Alpha Finance's ibETH token as one of our yield-generating strategies. This strategy tracks the value of its ibETH as ``ibETH.totalETH() / ibETH.totalSupply()`.

On May 9, 2021, Nipun Pitimanaaree, the lead Engineer at Alpha Finance published a blog providing more detail about the attack on Rari Capital.

https://nirup.medium.com/5-8-21-rari-capital-exploit-timeline-analysis-8bda31cbe1a

m Search

Get unlimited access to the best of Medium for less than \$1/week. [Become a member](#)

(5/8/21) Rari Capital Exploit Timeline & Analysis



Nirup Pitimanaaree · Follow
3 min read · May 9, 2021



17



1



Rari Exploiter address (same address as Value Defi exploiter on BSC):
<https://etherscan.io/address/0xch36b1ee0af68dce5578a487ff2da81282512233>

Exploiter net gain: ~2600 ETH (~\$10M)

On Saturday May 8th 1:48PM UTC, an exploiter started a series of transactions to Rari Capital's Ethereum Pool contract and was able to exploit ~2600 ETH in the process that lasted for ~50 minutes.

High-level Exploit Analysis

- Rari Capital's Ethereum Pool contract calculates the `ibETH/ETH` exchange rate by using the `ibETH.totalETH() / ibETH.totalSupply()` calculation from the `ibETH` contract, which can lead to incorrect assumption (e.g. during the `work` function call, where debt value gets updated towards the very end).
- `ibETH` is the interest-bearing ETH token on Alpha Homora, which represents user's share of the ETH lending pool.
- Alpha Homora is intentionally designed to support untrusted strategies, as long as certain invariant holds at the end (e.g., the position's collateral value > debt value).

Exploit & Action Timeline

- 1:48PM +UTC Rari Exploiter started executing the exploit
- 2:15PM +UTC We were notified about a suspicious transaction both by

This blog post specifically mentions the attackers Ethereum address:
`0xCB36b1ee0Af68Dce5578a487ff2Da81282512233`

An analysis of the transactions associated with this Ethereum address shows that consistent with the blog articles, between 05/08/2021 13:48 UTC and 05/08/2021 14:40 UTC, a sequence of transactions took place netting the attackers address with stolen ETH.

Poloniex

Thursday, September 12, 2024 12:20 PM

In November of 2023, Poloniex announced on their website that they were hacked.

https://support.poloniex.com/hc/en-us/articles/18976674677911-Announcement-on-Poloniex-Hack-Incident

Poloniex Links ▾ English (US) ▾ REQUEST HELP

POLONIEX

Hello! How can we help?

Search

Poloniex > News/Announcements > Latest Announcements

Announcement on Poloniex Hack Incident

Dear Poloniex users,

Regarding the Poloniex hack incident, we hereby promise to each Poloniex user that Poloniex maintains a healthy financial position and will fully reimburse the affected funds.

The Poloniex team has successfully identified and frozen a portion of the assets associated with the hacker's addresses to avoid further losses. At present, the losses are within manageable limits, and Poloniex's operating revenue can cover these losses.

Additionally, the team have restored Poloniex's systems, preserved relevant evidence, and in the coming days, we will work diligently to gradually resume deposits and withdrawals on Poloniex, ensuring 100% security. Apologize for any inconvenience this may have caused, thanks for your kind understanding and support!

Articles in this section

- Poloniex to Remove 16 Trading Pairs on June 4, 2024
- Poloniex Completes Upgrade of TP/SL Feature for Futures Trading
- Poloniex to Upgrade TP/SL Feature for Futures Trading
- September Giveaway: Enjoy Triple Rewards and Up to 20 USDT for Your Login!
- [PoR] Verification Snapshot Explained
- [PoR] How to Verify My Assets on Poloniex
- Bulk Asset Delistings November 7, 2024

Poloniex investor Justin Sun tweeted on November 10, 2023 that Poloniex suffered a hacking incident and that they were investigating:

https://x.com/justinsuntron/status/1722942733680296246

Settings

← Post

H.E. Justin Sun (hiring) @justinsuntron

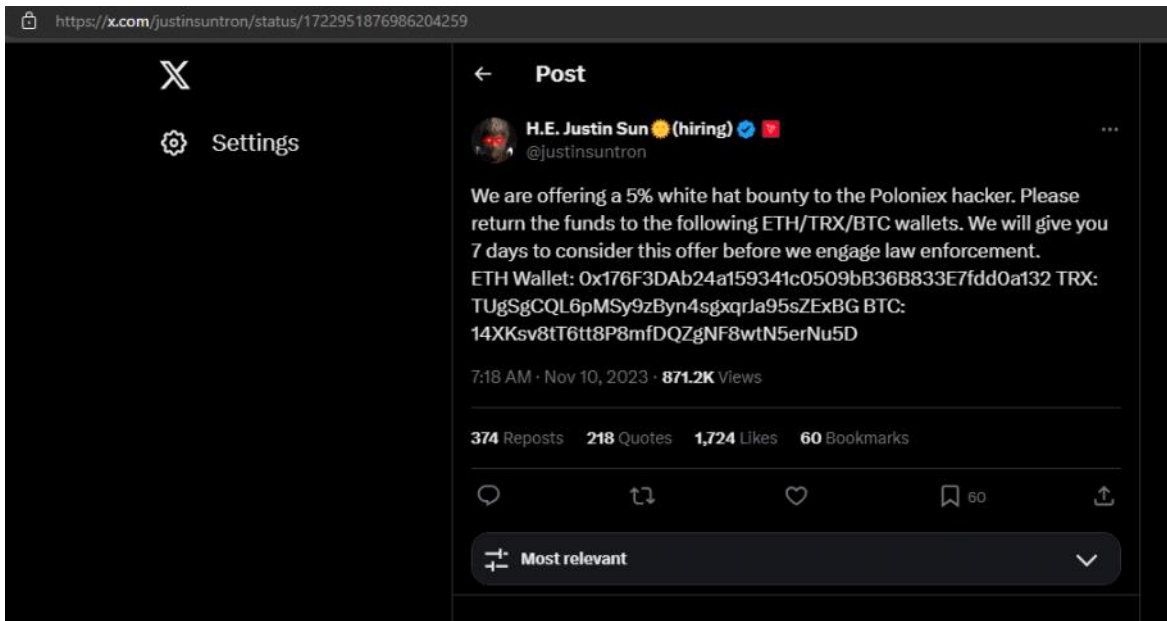
We are currently investigating the Poloniex hack incident. Poloniex maintains a healthy financial position and will fully reimburse the affected funds. Additionally, we are exploring opportunities for collaboration with other exchanges to facilitate the recovery of these funds.

6:42 AM · Nov 10, 2023 · 2M Views

327 Reposts 228 Quotes 1,586 Likes 50 Bookmarks

Most relevant

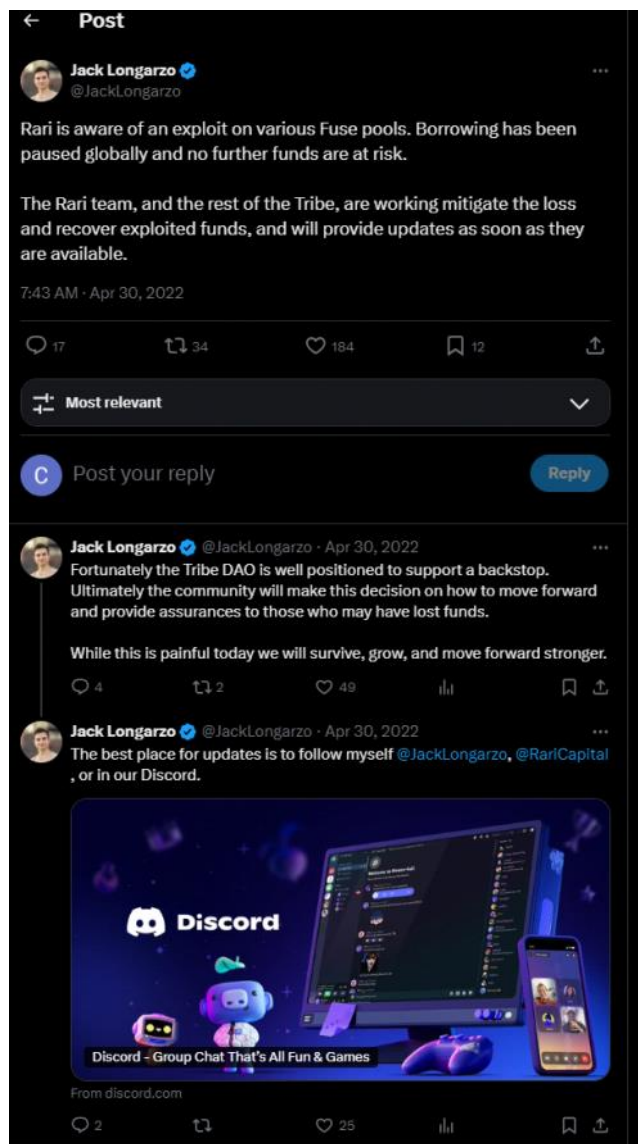
he was offering the Poloniex hacker a 5% white hat bounty.



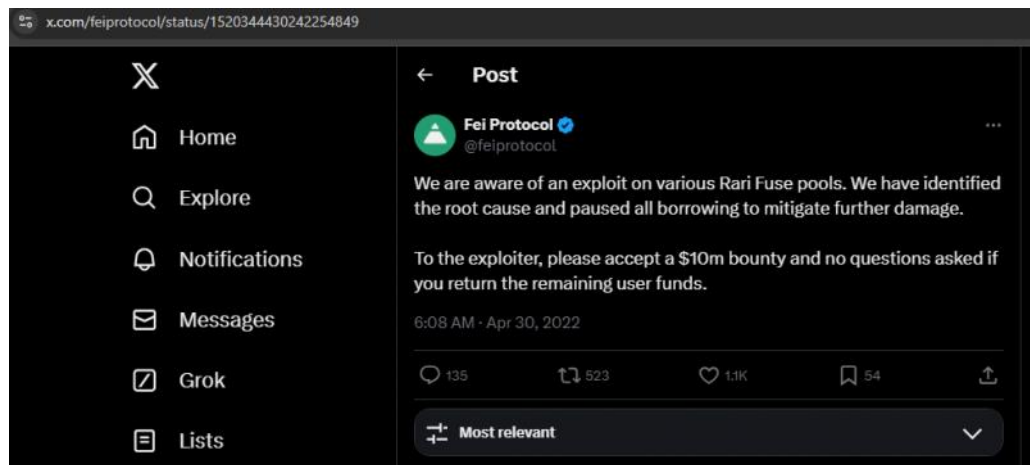
Rari / Fei 2022

Thursday, September 12, 2024 12:48 PM

On 04/30/2022, Jack Longarzo, a developer of Rari Capital, tweeted that Rari Capital was hacked:



The same day, the official Fei Protocol twitter handle posted a \$10 million no-questions-asked bounty for the return of funds.



Babylon Finance, a participant in the Rari fuse pool, released a Medium.com blog post describing the Rari attack:

medium.com/babylon-finance/babylon-lending-markets-fuse-fei-exploit-d8daa02c40b9



Containing the Fuse Exploit



Ramon Recuero · Follow

Published in Babylon.finance · 5 min read · May 2, 2022



161



Babylon is a community-led asset management protocol that enables users to create investment clubs (we call them gardens) and invest in DeFi together. It's built on the Ethereum network and it's non-custodial, transparent, permissionless, and governed by the community. BABL is the governance token behind it.



TLDR: Babylon was not hacked. Strategies that deposited into the fuse pool will be backstopped. There is going to be an on-chain proposal in FEI/Rari to refund the loss. If it doesn't go through, Babylon will cover it (up to its means). The goal is that no user funds will be affected.

On February 10th, we released the [Babylon Lending & Borrowing markets](#). The Babylon Gold lender pool on Rari allows Babylonians and garden strategies to deposit \$BABL as collateral and borrow assets from it.

Since its inception, the activity has been increasing until reaching more than \$8M in collateral and \$2M in borrowings.

On April 20th, Rari Fuse pools were hacked and more than \$70M was extracted.

The blog post goes on to reveal that the attacker's Ethereum address is 0x6162759edad730152f0df8115c698a42e666157f:

https://medium.com/babylon-finance/babylon-lending-markets-fuse-fei-exploit-d8daa02c40b9

n Q Search

The TVL in our Fuse Pool jumped from 8.7M to 46.8M and the borrowings increased from \$2.1M to \$43.7M 🤖

WTH happened? Shortly afterward we start looking at the transactions of our Comptroller markets on Etherscan and here there was:

<https://etherscan.io/tx/0x254735c6c14e4d338b1cc5bca43aab6b0f395ae06085013b1b2527180d270a31>

From: 0x6162759edad730152f0df8115c698a42e666157f (FeiProtocol-Fuse Exploiter) Contract: 0x320759ad9505047670180640c56763180d38e45

Interacted With (To):

- Transfer: 475,743,176,802,160,374,8 Ether From 0x6162759edad730152f0df8115c698a42e666157f To 0x6162759edad730152f0df8115c698a42e666157f
- Transfer: 475,743,176,802,160,374,8 Ether From 0x6162759edad730152f0df8115c698a42e666157f To 0x320759ad9505047670180640c56763180d38e45
- Transfer: 50,000 Ether From 0x320759ad9505047670180640c56763180d38e45 To 0x320759ad9505047670180640c56763180d38e45
- Transfer: 50,000 Ether From 0x320759ad9505047670180640c56763180d38e45 To 0x320759ad9505047670180640c56763180d38e45
- Transfer: 13,442,481,029,699,766,844,18 Ether From 0x6162759edad730152f0df8115c698a42e666157f To 0x320759ad9505047670180640c56763180d38e45
- Transfer: 13,442,481,029,699,766,844,18 Ether From 0x6162759edad730152f0df8115c698a42e666157f To 0x320759ad9505047670180640c56763180d38e45
- Transfer: 36,307,687,020,020,020,158 Ether From 0x6162759edad730152f0df8115c698a42e666157f To 0x320759ad9505047670180640c56763180d38e45
- Transfer: 50,000 Ether From 0x320759ad9505047670180640c56763180d38e45 To 0x320759ad9505047670180640c56763180d38e45
- Transfer: 475,743,176,802,160,374,8 Ether From 0x320759ad9505047670180640c56763180d38e45 To 0x320759ad9505047670180640c56763180d38e45

Tokens Transferred:

- From 0x6162759edad730152f0df8115c698a42e666157f To 0x6162759edad730152f0df8115c698a42e666157f For 249,729,732,600,627,552,407,976,982 (Babylon's Go, (DAI-1...))
- From 0x6162759edad730152f0df8115c698a42e666157f To 0x6162759edad730152f0df8115c698a42e666157f For 50,000,000 (\$50,150,000.00) (Dai Stablecoin, (DAI))
- From 0x6162759edad730152f0df8115c698a42e666157f To 0x6162759edad730152f0df8115c698a42e666157f For 249,729,732,600,627,552,407,976,982 (Babylon's Go, (DAI-1...))
- From 0x6162759edad730152f0df8115c698a42e666157f To 0x320759ad9505047670180640c56763180d38e45 For 50,000,000 (\$50,150,000.00) (Dai Stablecoin, (DAI))
- From 0x320759ad9505047670180640c56763180d38e45 To 0x6162759edad730152f0df8115c698a42e666157f For 182,892,969,489,866,340,705,763 (Babylon's Go, (ETH-1...))
- From 0x320759ad9505047670180640c56763180d38e45 To Balancer Vault For 50,000 (\$136,834,000.00) (Wrapped Ether, (WETH))
- From 0x320759ad9505047670180640c56763180d38e45 To Balancer Vault For 50,000,000 (\$50,150,000.00) (Dai Stablecoin, (DAI))
- From 0x320759ad9505047670180640c56763180d38e45 To 0x393c439666f5 For 963,852,736,643,151,175,735,955 (\$966,744.32) (Dai Stablecoin, (DAI))
- From 0x320759ad9505047670180640c56763180d38e45 To 0x393c439666f5 For 717,230,862,073,915,275,731,69 (\$718,665.32) (Frax (FRAX))
- From 0x320759ad9505047670180640c56763180d38e45 To 0x393c439666f5 For 483,252,880,527,706,893,985,44 (\$482,131.62) (Frax (FRAX))

The following account [0x6162759edad730152f0df8115c698a42e666157f](https://etherscan.io/address/0x6162759edad730152f0df8115c698a42e666157f) managed to extract \$3.41M of collateral from our Fuse Pool between ETH, DAI, FRAX and FEI.

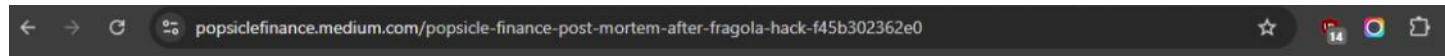
Three Babylon gardens had strategies active on the Fuse Pool: 🌿 The Fountain of ETH, 💰 The Stable Garden, and Stable Pebble. Immediately, we took the following measures:

An analysis of this Ethereum address shows activity consistent with an attack on FeiProtocol:

Popsicle

Friday, September 13, 2024 12:35 PM

On 8/4/2021, Popsicle Finance posted on their official Medium.com blog account that they had been hacked on 08/03/2021.



Medium

Search

Write



Get unlimited access to the best of Medium for less than \$1/week. [Become a member](#)

Popsicle Finance Post Mortem-After Fragola Hack



Popsicle.Finance (WAGMI) · Follow

5 min read · Aug 4, 2021

370

1



This post is not something that we thought we would ever have to write and not something that is fun to announce, however as we know yesterday at 10:53 PM UTC time a hacker executed a transaction that managed to drain 85% of the Sorbetto Fragola (UniswapV3 Optimizer) pools.

This has only affected the Sorbetto Fragola contracts, other contracts such as nICE staking, ICE farming contracts and ICE token contracts are not affected.

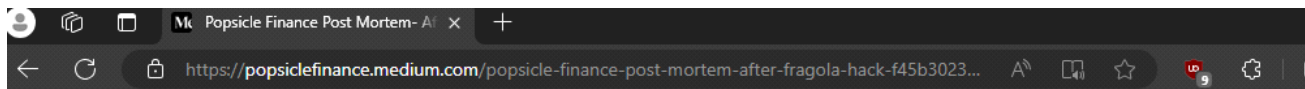
Check out the Hackers Transaction [here](#).

Funds lost:

Currency	Amount
wETH	2.6k
USDC	5M
USDT	5M
DAI	160k
UNI	10k
wBTC	96
Total	\$20.7M

What actually happened?

This post stated that the hacker stole tokens, swapped them for Ether, and then cashed out at Tornado Cash:



The hacker made the contract believe that he earned as many fees as the total TVL of the pool and thus is entitled to the \$20.7m that was in the pool. This hack was only possible because everything happened within one transaction (due to flashloan).

The hacker took all these captured coins and first swapped them for ETH on Uniswap, and thereafter put them through Tornado.Cash to launder them.

- [Swap Transaction 1](#)
- [Swap Transaction 2](#)
- [Swap Transaction 3](#)
- [Swap Transaction 4](#)
- [Swap Transaction 5](#)

Sadly, neither we nor our 2 editors (Peckshield & Certik) noticed this bug.

For an in-depth look and analysis of the code, you can refer to this analysis by our friends [@blocksecteam](#) in the article [here](#).

So, now what?

First of all, we would like to address the black hat hacker. **Although this may be a long shot we are offering a completely clean \$1,000,000 bounty paid in whatever currency he/she likes if funds are returned.**

We are all working here in the new and exciting DeFi space, having people that find vulnerabilities is a part of the ecosystem, however in order to not scare people away we need to make sure they can trust the space. Returning the funds will show the strength of this crypto community.

[@danielesesta](#) [@squirrelcrypto](#) [@popsiclefinance](#) Twitter DMs are open to start the conversation.

The blog post links to the Etherscan transaction which is shown when hovering over the link. The hacker's transaction hash was 0xcd7dae143a4c0223349c16237ce4cd7696b1638d116a72755231ede872ab70fc.

Check out the Hackers Transaction [here](#).

Funds lost:

Currency	Amount
wETH	2.6k
USDC	5M
USDT	5M
DAI	160k
UNI	10k
wBTC	96
Total	\$20.7M

What actually happened?

You can find the Transaction flow [here](#).

In order to start the explanation let's first explain how Fragola actually works.

1. Funds from the user go straight to UniV3.
<https://etherscan.io/tx/0xcd7dae143a4c0223349c16237ce4cd7696b1638d116a72755231ede872ab70fc>

An analysis of this transaction shows that the transaction was ordered by malicious Ethereum address 0xf9E3D08196F76f5078882d98941b71C0884BEa52.

xToken

Tuesday, September 17, 2024 3:34 PM

On May 12, 2021, the founder of xToken posted on xToken's official Medium.com page that they suffered a hack.

Medium  Search

✦ Get unlimited access to the best of Medium for less than \$1/week. [Become a member](#)

Initial Report on xBNTa, xSNXa Exploit



michael.j.cohen · [Follow](#)

Published in xToken · 4 min read · May 12, 2021

 523



An attacker exploited the xBNTa and xSNXa contracts at 9:44 am EST today (May 12). The contracts were exploited simultaneously within a single transaction and the xBNTa Bancor pool as well as the xSNXa Balancer pool were immediately drained. We noticed price and supply discrepancies on our frontend about ten minutes later and several community members alerted us around this time as well. Minting on all xToken contracts was paused by 10:14 am.

We are deeply, deeply sorry for the loss of funds and are exploring the best path forward. Total value lost on the Bancor and Balancer liquidity pools was about ~\$25m across several assets. Total value lost directly on the xSNXa contract was 416 ETH. No value was lost directly on the xBNT contract.

While the attacker minted large amounts of xBNT and xSNX supply in order to drain the liquidity pools, **all of the BNT and SNX remains in the xToken contracts**. That said, 416 ETH was extracted from the xSNX contract (the xSNX contract holds ETH as part of a debt-hedging strategy).

xBNTa Exploit

Our xBNT contract allows investors to mint xBNT with ETH. The contract exchanges the ETH for BNT on Bancor and uses the BNT acquired to calculate the correct amount of xBNT to mint. We pass a trade “path” via a

The blog posts mentions that the contracts were stolen in a single transaction. I analyzed that transaction in Etherscan.

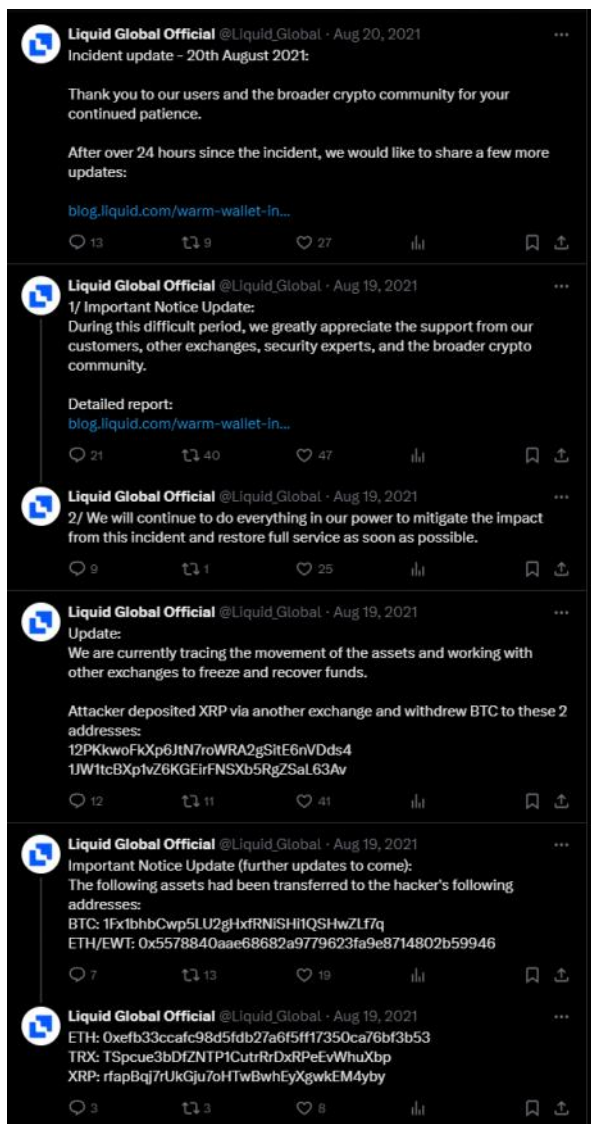
Liquid.com

Tuesday, September 17, 2024 4:18 PM

On 08/18/2021, Liquid.com exchange announced on Twitter that they had been hacked:



Liquid.com continued to update its Twitter followers about the hack. On 08/20/2021 they Tweeted a link to a blog post on liquid.com. That blog post no longer exists.



Using archive.org, I recovered a version of this blog post from 08/20/2021. In the post, they explain details of the hack -- approximately \$91.35 million of cryptocurrency was stolen comprising 69 different crypto assets.



(disabled for onchain movement) due to the assistance of the crypto community and other exchanges.

- 69 different crypto assets were misappropriated and sent to other exchanges or defi swapping venues.
- Assets placed in Liquid Earn are not impacted.

Liquid's teams are still assessing the attack vector used and taking measures to mitigate the impact to users.

More information will be provided as it becomes available via Liquid Help Center & Liquid Global Twitter.

During this difficult period we greatly appreciate the support from our customers, other exchanges, security experts, and the broader crypto community. Liquid will continue to do everything in its power to mitigate the impact from this incident and restore full service as soon as possible.

These are the list of known addresses used by the un-authorised party:

Currency	Wallet Address
BTC	1Fx1bhbCwp5LU2gHxfRNiSHi1QSHwZLf7q
ETH/ERC-20	0x5578840aae68682a9779623fa9e8714802b59946
ETH	0x8762db106b2c2a0bccb3a80d1ed41273552616e8
ETH	0xefb33ccafc98d5fdb27a6f5ff17350ca76bf3b53
ETH	0xca0e7269600d353f70b14ad118a49575455c0f2f
TRX	TSpcue3bDfZNTp1CutrrDxRPeEvWhuXbp
XRP	rfapBqj7rUkGju7oHTwBwhEyXgwkEM4yby

The blog specifies the ETH/ERC20 addresses used to steal funds:

0x5578840aae68682a9779623fa9e8714802b59946
 0x8762db106b2c2a0bccb3a80d1ed41273552616e8
 0xefb33ccafc98d5fdb27a6f5ff17350ca76bf3b53
 0xca0e7269600d353f70b14ad118a49575455c0f2f

Ether Heist

Ethereum address 0xefb33ccafc98d5fdb27a6f5ff17350ca76bf3b53 received approximately 538 ETH on 08/19/2021 01:14 UTC consistent with the blog post. On 07/18/2022 09:28 UTC, approximately 538 ETH was transferred to address 0xE88243506Fcc79052d85ad449ef6A02ACE51c3c6 on 07/18/2022 09:28 UTC.

MGNR.io

Wednesday, September 18, 2024 3:02 PM


On October 13, 2021, the official Twitter account of mgnr.io (@mgnr_io) announced that they had been hacked on October 8, 2021. The tweet has been deleted, but I was able to find a copy of it:

https://web.archive.org/web/20211014032211/https://twitter.com/mgnr_io/status/1448489258029703168/

https://web.archive.org/web/20211014032211/https://twitter.com/mgnr_io/status/1448489258029703168/

com/mgnr_io/status/1448489258029703168/


Nov 2022



mgnr.io
@mgnr_io
quantitative algorithmic hustle
trading dot com
mgnr.io
Joined August 2020

mgnr.io @mgnr_io · 8s
0 /

h A c K e D



1

mgnr.io @mgnr_io · 7s
1 /

as some of you are already aware

on 8 october @mgnr_io was the victim of a malicious and targeted cyber attack

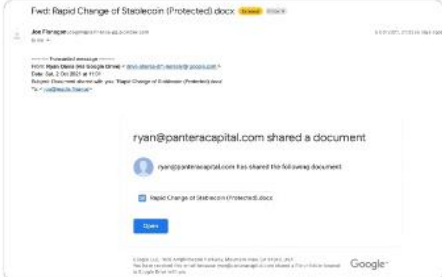
the attackers appear to be very sophisticated and have scripting abilities / facility with cross-chain bridging and mixing techniques

1

mgnr.io @mgnr_io
2 /

the point of entry was likely a phishing email masked as somebody we recognized from @maplefinance and containing a fake docx from @PanteraCapital

we've subsequently heard of 2 other crypto firms receiving an equally targeted attacks (also with 'pantera' term sheets)



8:22 PM · 13 Oct 2021

1

mgnr.io @mgnr_io · 8s
3 /

the intrusion was probably used to implant a key logger and steal credentials to a password manager where we had (stupidly) shared a privkey as temporary hot wallet between a few team members

1

On October 8, 2021, the mgnr.io team made a complaint with FBI Los Angeles stating that they were hacked and that approximately \$35 million worth of cryptocurrency was stolen and sent to Ethereum

bZx

Wednesday, September 18, 2024 4:41 PM

On 11/05/2021, bZx published a "Preliminary Post Mortem" on their official website. The website has been since deleted, but I recovered a copy from archive.org.

The screenshot shows a web browser displaying the 'Preliminary Post Mortem' article from bZx, archived on September 18, 2024. The browser's address bar shows the URL: <https://web.archive.org/web/20220126183731/https://bzx.network/blog/preliminary-post-mortem>. The page header includes the Internet Archive logo, the URL, and navigation links for 'Developers' and 'Help Center'. The article title is 'Preliminary Post Mortem'. The main text states: 'We are still investigating, as new information comes to light and unfolds, we will update this post with new information.' It includes a 'Summary' section describing a phishing attack on a bZx developer's private keys, which affected BSC and Polygon deployments but not the Ethereum protocol. A 'Who was affected?' section lists: a bZx Developer; lenders, borrowers, and farmers on Polygon and BSC; and funds removed from BSC and Polygon. An 'Impact and Funds Stolen' section includes a note: 'We are investigating further to determine the amount of funds that were stolen. We will update the article once the values have been calculated.' and a list of events: the hacker stole BZRX on BSC and Polygon; BZRX on Ethereum was not affected; and funds on Polygon and BSC were drained.

Preliminary Post Mortem

We are still investigating, as new information comes to light and unfolds, we will update this post with new information.

Summary

A bZx developer had his personal wallet's private keys taken in a phishing attack. The phishing attack was similar to one that affected another user recently named "mgrn.io".

The ethereum deployment of bZx protocol is safe following the compromise of an individual bZx developer's computer and their private keys. The Ethereum bZx protocol itself wasn't exploited. Since bZx Protocol on ethereum is governed by a DAO, the ethereum implementation was not affected. Ethereum Governance is also unaffected.

This attack granted the hacker access to the content of the bZx Developers wallet, and also the private keys to the BSC and Polygon deployment of bZx Protocol. After gaining control of BSC and Polygon the hacker drained the BSC and Polygon protocol, then upgraded the contract to allow draining of all tokens that the contracts had given unlimited approval.

Who was affected?

- A bZx Developer
- Lenders, borrowers, and farmers with funds on Polygon and BSC, and those who had given unlimited approvals to those contracts. We are gathering data on the specific wallets which were affected by the attack.
- Funds were also removed from the BSC and Polygon implementation of the protocol.

Impact and Funds Stolen:

_Note: We are investigating further to determine the amount of funds that were stolen. We will update the article once the values have been calculated. _

- The hacker stole BZRX on BSC and Polygon using the private key then deposited some of the stolen BZRX funds to be used as collateral to borrow against other funds on the protocol.
- BZRX deployment on Ethereum was not affected and no funds were stolen.
- Funds held in the Polygon and BSC deployment were drained.

The Post Mortem states that bZx developer was hacked and cryptocurrency was stolen starting on 11/05/2021 11:07 UTC. Various tokens on BSC and Polygon were stolen.

The blog post identifies the following Ethereum addresses as belonging to the hacker to include the following:

0x967BB571F0Fc9Ee79c892aBF9f99233AA1737E31
 0x0ACC0e5faA09Cb1976237c3a9aF3D3d4b2f35FA5
 0x1Ae8840cEaEf6EeC4dA1b1e6e5FCf298800b46e6

Ox74487eEd1E67F4787E8C0570E8D5d168a05254D4
 OxAfad9352eB6Bcd085Dd68268D353d0ed2571aF89

web.archive.org/web/20220126183731/https://bzx.network/blog/preliminary-post-mortem

Internet Archive Wayback Machine 30 captures 6 Nov 2021 - 31 May 2022

Developers Help Center

- Working with Exchanges and investigators to identify the hacker.
- Relaunching Polygon and BSC implementations under DAO control.
- Contact ISP/VPN Provider
- DAO Developing compensation plan for affected users that is appropriate and necessary after the amount lost is calculated and efforts are made to recover funds.

Hacker Wallet Balances:

Polygon

- Oxafad9352eb6bcd085dd68268d353d0ed2571af89
 - 2M BZRX

BSC:

- Ox74487eed1e67f4787e8c0570e8d5d168a05254d4
 - 10M BZRX
- Ox967bb571f0fc9ee79c892abf9f99233aa1737e31
 - 2.5M BZRX
- Ox0ACC0e5faA09Cb1976237c3a9aF3D3d4b2f35FA5
 - Hackers Primary Wallet on BSC used in attack

Ethereum

- Ox74487eed1e67f4787e8c0570e8d5d168a05254d4
 - 10M BZRX
- Ox967bb571f0fc9ee79c892abf9f99233aa1737e31
 - 12M VBZRX
- Ox967bb571f0fc9ee79c892abf9f99233aa1737e31
 - 82K BZRX
- Ox74487eEd1E67F4787E8C0570E8D5d168a05254D4
 - \$4m in ETH
 - Main Hackers wallet
- Ox1ae8840ceaf6eec4da1b1e6e5fcf298800b46e6
 - Hackers wallet
 - USDT Frozen

Consistent with the blog post, an analysis of these five Ethereum addresses shows large token transfers from bZx wallets and subsequent swaps and liquidations to Ether.

Approximately 9,315 ETH valued at about \$39.36 million was sent from these Ethereum addresses to an intermediary Ethereum wallet 0x20d9e73aaf69a3cd66ad7477de7358d0ed44b10 in a series of transactions between 11/15/2021 14:09 UTC and 12/13/2021 05:37 UTC.

An analysis of 0x20d9e73aaf69a3cd66ad7477de7358d0ed44b10 shows that between 11/15/2021 02:14 UTC and 12/13/2021 06:08 UTC, in a series of transactions, approximately 10,960 ETH was transferred to Tornado Cash wallet 0x722122df12d4e14e13ac3b6895a86e84145b6967. The approximate value of this ETH was \$45.94 million.

Qubit Finance

Monday, September 23, 2024 1:05 PM

On 01/28/2022, Qubit Finance announced on their official Medium.com blog that their protocol was exploited and funds were stolen. The blog stated that the attack began around 01/27/2022 09:18 UTC:

Sign in

Protocol Exploit Report. The Qub

https://medium.com/@QubitFin/protocol-exploit-report-305c34540fa3

Medium Search Write Sign up Sign in

Protocol Exploit Report

Qubit Finance · Follow
2 min read · Jan 28, 2022

72 1

The Qubit protocol was subject to an exploit to our QBridge deposit function.

This report includes an analysis of the attack in its entirety in order to ascertain the nature of the exploit and, to prevent any similar exploits in the future.

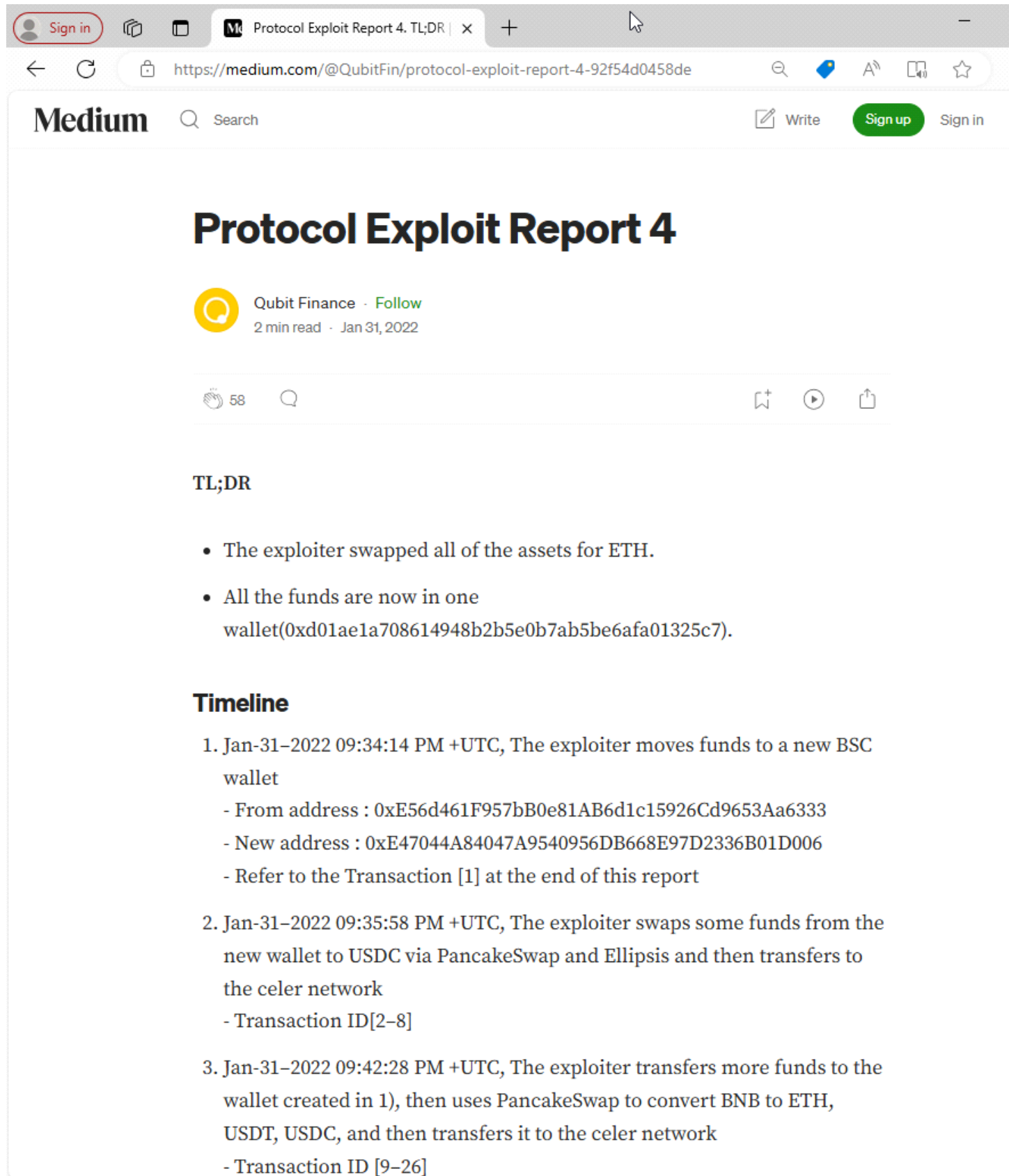
Incident Timeline

1. Jan-27-2022 09:18:55 PM +UTC: 0.8887725 ETH sent from tornado to attacker account
2. Jan-27-2022 09:34:01 PM +UTC~Jan-27-2022 09:50:41 PM +UTC : Sent 16 deposit tx to QBridge of Ethereum
3. Jan-27-2022 09:36:32 PM +UTC~Jan-27-2022 09:51:02 PM +UTC : Sent 16 voteProposal tx to QBridge contract of BSC by Qubit Relayer
4. A number of xETH tokens were minted by 16 voteProposal tx, and liquidity in Qubit was withdrawn using this as collateral

Exploit Method

The attacker called the QBridge deposit function on the ethereum network, which calls the deposit function QBridgeHandler.

In the days following the exploit, the Qubit team made additional updates on Medium on the status of the stolen funds. In a blog post dated 01/31/2022, Qubit posts that the exploiter swapped all the stolen assets for Ether and the funds are in wallet 0xd01ae1a708614948b2b5e0b7ab5be6afa01325c7:



Protocol Exploit Report 4

Qubit Finance · Follow
2 min read · Jan 31, 2022

58

TL;DR

- The exploiter swapped all of the assets for ETH.
- All the funds are now in one wallet(0xd01ae1a708614948b2b5e0b7ab5be6afa01325c7).

Timeline

1. Jan-31-2022 09:34:14 PM +UTC, The exploiter moves funds to a new BSC wallet
 - From address : 0xE56d461F957bB0e81AB6d1c15926Cd9653Aa6333
 - New address : 0xE47044A84047A9540956DB668E97D2336B01D006
 - Refer to the Transaction [1] at the end of this report
2. Jan-31-2022 09:35:58 PM +UTC, The exploiter swaps some funds from the new wallet to USDC via PancakeSwap and Ellipsis and then transfers to the celer network
 - Transaction ID[2-8]
3. Jan-31-2022 09:42:28 PM +UTC, The exploiter transfers more funds to the wallet created in 1), then uses PancakeSwap to convert BNB to ETH, USDT, USDC, and then transfers it to the celer network
 - Transaction ID [9-26]

An analysis of Ethereum address 0xd01ae1a708614948b2b5e0b7ab5be6afa01325c7, shows that

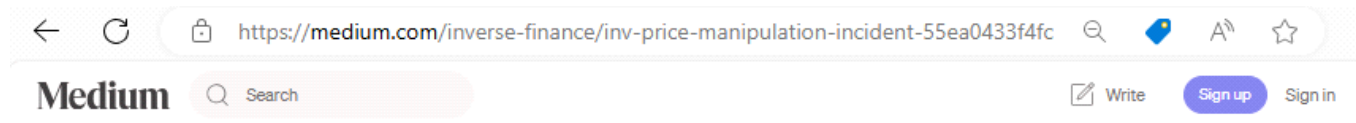
consistent with the blog article, this address received approximately 21,044 ETH valued at \$55.07 million between 01/29/2022 15:26 UTC and 01/31/2022 23:39 UTC.

Between 02/07/2022 17:55 UTC and 02/07/2022 18:43 UTC, 7,500 of this ETH valued at approximately \$23.56 million was liquidated through Tornado Cash wallet 0x722122df12d4e14e13ac3b6895a86e84145b6967.

Inverse Finance

Monday, September 23, 2024 2:57 PM

On 04/04/2022, a blog post titled "INV Price Manipulation Incident" was posted by the official Inverse Finance account on Medium.com. That article stated that on 04/02/2022, Inverse Finance had approximately \$15.6 million in cryptocurrency stolen through a market manipulation exploit.



INV Price Manipulation Incident



patb · Follow

Published in Inverse Finance · 4 min read · Apr 4, 2022



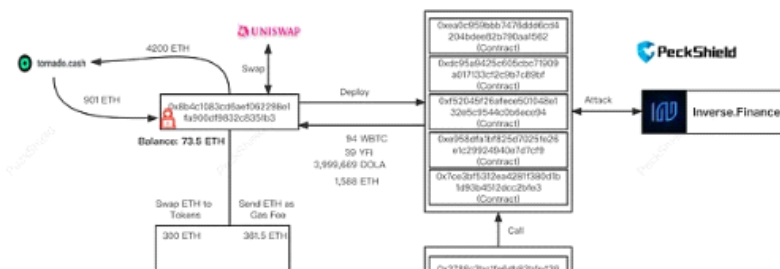
What Happened

On Saturday (April 2nd) the Keep3r TWAP oracle for INV was manipulated using a capital-intensive manipulation of the INV/WETH price oracle on Sushiswap, resulting in a sharp rise in the price of INV which subsequently enabled the attacker to borrow \$15.6 million in DOLA, ETH, WBTC, & YFI. The manipulation was not a flash loan attack and was not related to Inverse's smart contract or front end code, but rather an error in the TWAP oracle sampling method.

Details of the Price Manipulation

(h/t <https://twitter.com/peckshield>)

1. At approx. 08:00 EDT on April 2, 2022 attacker withdrew 901 ETH from Tornado Cash and made a series of trades primarily in the INV/DOLA pool on SushiSwap. This pool maintained relatively light liquidity compared to INV liquidity, for example, on Coinbase.



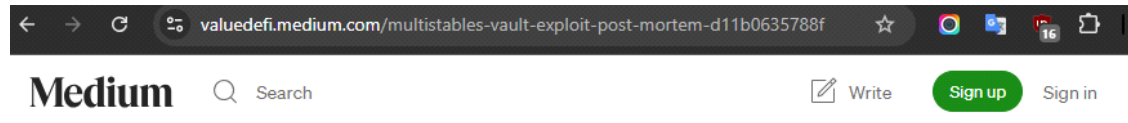
According to the blog post, the stolen funds were transferred to Ethereum address 0x8b4c1083cd6aef062298e1fa900df9832c8351b3.

An analysis of Ethereum address 0x8b4c1083cd6aef062298e1fa900df9832c8351b3 shows that consistent with the blog post, between 04/02/2022 11:04 UTC and 04/02/2022 11:09 UTC the address received 1,588 ETH and a large amount of WBTC, YFI, and DOLA tokens.

ValueDefi

Monday, September 23, 2024 4:47 PM

On 11/15/2020, Value DeFi posted on their official Medium.com blog page that they were exploited by a hacker on 11/14/2020 15:36 UTC resulting in a loss of approximately \$6 million.



MultiStables Vault Exploit Post-Mortem



Value DeFi Protocol · Follow

5 min read · Nov 15, 2020



441



2



Summary:

The ValueDeFi MultiStables vault was recently the subject of a complex attack that resulted in a loss of user deposits. What follows below is a post-mortem analysis and a description of proposed actions to mitigate economic impact on the community.

The Incident:

On Nov 14th 2020 at 03:36:30 PM UTC, a hacker performed a flash-loan exploit on the MultiStables vault of ValueDeFi protocol, which resulted in a net loss of roughly 6mil\$.

The new vault uses our new code of vault v2, which had not been audited.

The blog post details the transaction hash of the exploit as 0x46a03488247425f845e444b9c10b52ba3c14927c687d38287c0faddc7471150a. An analysis of this transaction, shows that it is from address 0xa773603b139Ae1c52D05b35796DF3Ee76D8a9A2F.

Thorchain

Monday, September 23, 2024 5:55 PM

On 07/30/2021, the Thorchain official Medium.com account published a blog post titled "Post-mortem: ETH Router Exploits 1 & 2, and premature Return to Trading Incident". In the blog post, Thorchain claims they were exploited resulting in a loss of crypto assets.

The article details that the attacker's wallet is 0x8c1944FAC705ef172f21f905b5523Ae260F76d62.

<https://medium.com/thorchain/post-mortem-eth-router-exploits-1-2-and-premature-return-to-trading-incident-2908928c5fb>

Post-mortem: ETH Router Exploits 1 & 2, and premature Return To Trading Incident

The ETH Router Exploit 1 & 2, Premature Trading, fixes and network response, as well as the 5 Pronged Response.

THORChain · Follow
Published in THORChain · 7 min read · Jul 30, 2021

251
 1

Summary

THORChain suffered two back to back exploits on its ETH Router. The first took all the ETH from the system via an attack contract that sat in front of the Router, and the second took all the economically significant ERC20s via an attack contract that sat behind the router.

In both cases the exploits were able to trick the Bifrost into reporting receiving assets it had not. The root cause was a Bifrost interface that did not fully account for the degrees of manipulation that can occur in smart contract events.

No other chains or assets were affected.

The THORChain team and community have kicked off a 5-Pronged Plan to address, fix and recover. They are detailed below.

The THORChain treasury will cover all losses to LPs. Nodes are not affected.

Exploit 1 — ETH

The attacker deployed a contract that sat in front of the Router, which was able to call the `deposit()` function of the Router. The ability for the Router to be wrapped was [recently made available to support ecosystem development](#).

The write-ups state that the hacker was able to net various ERC-20 tokens to include USDT, XRUNE, and SUSHI resulting in a loss of approximately \$8 million.

An analysis of the wallet shows that consistent with the post-mortem, various ERC-20 tokens are transferred from Thorswap into the attacker's address between 07/22/2021 19:00 UTC and 21:42 UTC. These tokens were then swapped for approximately 1,934 ETH using SushiSwap and Uniswap on 07/22/2021 22:27 UTC.


AFKFinance

Tuesday, September 24, 2024 9:53 AM

In September 2021, there were reports that AFK Systems conducted a "rug pull" stealing \$12 million of its users' funds. The rug pull happened on 09/10/2021.

Here is one blog post detailing the rug pull:

<https://www.publish0x.com/make-money-private-again/afk-systems-con-job-and-safety-of-defi-protocols-xmpoke>



AFK Systems Con Job and Safety of DeFi Protocols

By Didacus | [Make Money Private Again!](#) | 19 Sep 2021

\$0.66

On 10 September 2021 a recently established Polygon farm, AFK System, stole over 12 million USD of users' funds and deleted any footprint on the web and social media. Funds in AFK farms, linked to AFK two Masterchef smart contracts

<https://polygonscan.com/address/0x6A08491e01b36D116c332C87253a78e6480f7f6D>

<https://polygonscan.com/address/0xbb3f43008e277543353588ca2a4941f12e3cacc0>

were emptied and laundered via Tornado Cash. This is a summary of the events with relevant links.

From OBELISK AUDIT TRANSCRIPT at
<https://twitter.com/ObeliskOrg/status/14364938981809315881>. On August 21, AFKsystem contacted Obelisk to audit their blockchain contracts. The audit began in early September.

2. During the audit we found multiple instances of errors that could be used maliciously. As part of the audit process,

The same author of the blog post wrote a template police report for victims.

AFK Systems Con Job and Safety of DeFi Protocols

By Didacus | Make Money Private Again! | 19 Sep 2021

\$0.66

On 10 September 2021 a recently established Polygon farm, AFK System, stole over 12 million USD of users' funds and deleted any footprint on the web and social media. Funds in AFK farms, linked to AFK two Masterchef smart contracts

<https://polygonscan.com/address/0x6A08491e01b36D116c332C87253a78e6480f7f6D>

<https://polygonscan.com/address/0xbb3f43008e277543353588ca2a4941f12e3cacc0>

were emptied and laundered via Tornado Cash. This is a summary of the events with relevant links.

From OBELISK AUDIT TRANSCRIPT at

<https://twitter.com/ObeliskOrg/status/14364938981809315881>.

On August 21, AFKsystem contacted Obelisk to audit their blockchain contracts. The audit began in early September.

2. During the audit we found multiple instances of errors that could be used maliciously. As part of the audit process, a first draft was sent to AFKsystem with proposals to solve the problems.

3. On September 11 AFK (September 10 UTC), AFKsystem withdrew the funds deposited in the middle of the audit. It is important to emphasize that a project in the middle of an audit process is still



According to this author, the stolen funds were deposited into Ether address 0x56eb4a5f64fa21e13548b95109f42fa08a644628.

Similarly, an online post by the Quadriga Initiative, a self-described "community-based, not-for-profit crypto watchdog & fraud recovery platform" details the mechanics of the AFK system fraud:



DESCRIPTION OF EVENTS

"AFKsystem.Finance is a Decentralized Yield Farming Ecosystem created by Yield Farmers, for Yield Farmers. Our \$SILVER token ensures that AFKsystem.Finance is owned by its users. \$SILVER will only be rewarded to users who benefit the protocol, thus there will be no single asset farming pools, only single asset Missions (AAVE Vaults)." "[T]he address used in the [contract] was filled using tornado[cash]" on July 8th.

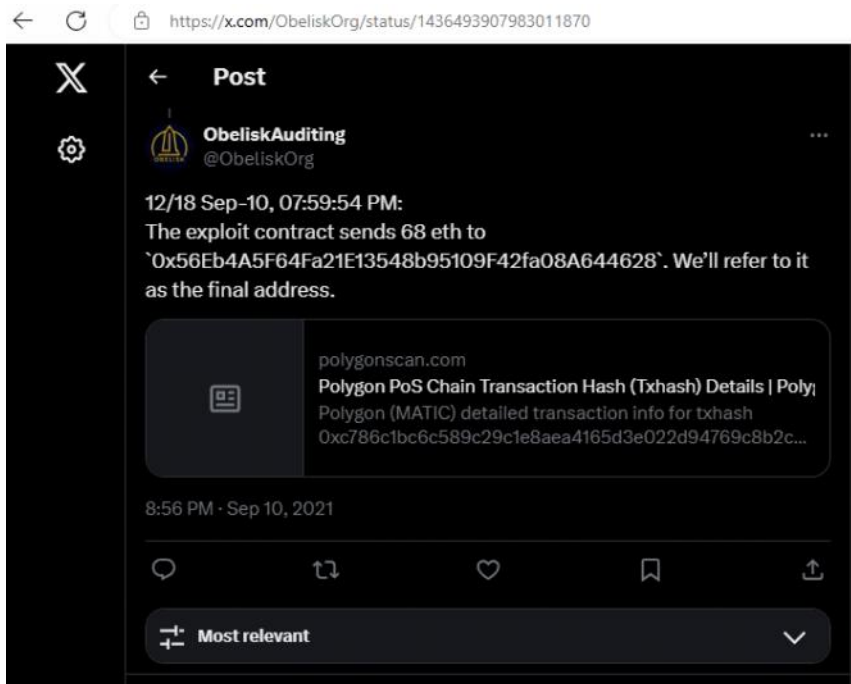
"AFKsystem.Finance launching in less than 24 hours, Polygon newest DeFi Yield Vaults! Partnered with Dfyn exchange, join us at our launch on 19th Aug UTC 2PM! Fairly Launched!"

"Our official auditing partner, @OxPaladinSec, has funnily always pointed out these governance privileges to change the router as either high severity or medium severity." "AFK Systems cancelled their Paladin audit in favor of another auditor."

"On the 21st of August, AFK contacted Obelisk for an audit of their smart contracts. The actual audit started at the beginning of September."



ObeliskAuditing, who claims to be the independent auditor of AFKsystem also published a post-mortem in a Twitter thread. They traced the stolen funds and also reported the recipient address as 0x56eb4a5f64fa21e13548b95109f42fa08a644628.



An analysis of the Ethereum address 0x56eb4a5f64fa21e13548b95109f42fa08a644628 shows that consistent with the public reporting, on 09/10/2021 22:01 UTC approximately 2,834,436 DAI tokens are deposited into the address from the Polygon Matic Bridge.

Etherscan Home Blockchain Tokens NFTs Resources Developers More | Sign In

Address 0x56Eb4A5F64Fa21E13548b95109F42fa08A644628 Buy Exchange Play Gaming

Sponsored: Metawin: Win 3 ETH worth \$7k+! Grab Your FREE ENTRY Today. [Enter Here.](#)

Warning: This address is reported to have been involved in a rug pull of AFKSystem.

Overview

ETH BALANCE
0.31299168728416728 ETH

ETH VALUE
\$823.32 (@ \$2,630.49/ETH)

TOKEN HOLDINGS
\$0.00 (3 Tokens)

More Info

PRIVATE NAME TAGS
[+ Add](#)

TRANSACTIONS SENT
Latest: 1137 days ago First: 1202 days ago

FUNDED BY
0xf49ab880...5B7411fa7 at txn 0x5ef20dda814...

Multichain Info

\$1,807 (Multichain Portfolio)

2 addresses found via Blockscan

Transactions Internal Transactions **Token Transfers (ERC-20)** NFT Transfers Analytics Multichain Portfolio Cards New

Advanced Filter

Transactions involving tokens marked as suspicious, unsafe, spam or brand infringement are currently hidden. To show them, go to [Site Settings](#).

Transactions with zero token value are currently hidden. To show them, go to [Site Settings](#).

Latest 2 ERC-20 Token Transfer Events

Transaction Hash	Method	Block	Date Time (UTC)	From	To	Amount	Token
0x263aab8531...	Multicall	13200597	2021-09-10 22:03:07	0x56Eb4A5F...08A644628	OUT Uniswap V3: DAI-USDC	2,834,436.7717075	Dai Stableco... (DAI)
0xd9cf15c9b2f...	Exit	13200586	2021-09-10 22:01:20	Polygon (Matic): ERC20	IN 0x56Eb4A5F...08A644628	2,834,436.7717075	Dai Stableco... (DAI)

[Download: CSV Export]

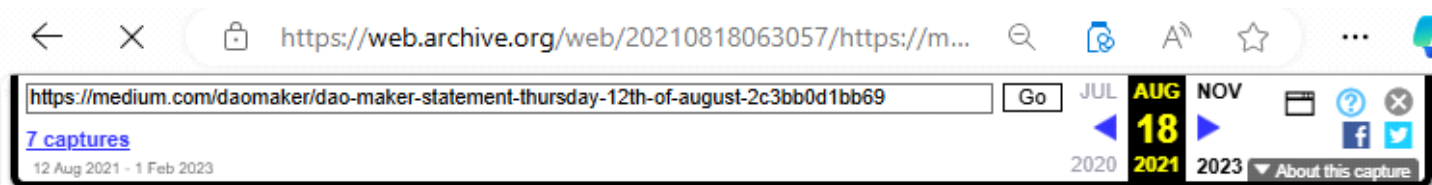
A wallet address is a publicly available address that allows its owner to receive funds from another party. To access the funds in an address, you must have its private key. Learn more about addresses in our Knowledge Base.

On 09/10/2021 22:03 UTC, the total balance of DAI is swapped for approximately 879 ETH using Uniswap.

DAO Maker

Tuesday, September 24, 2024 11:18 AM

On 08/12/2021, DAO Maker published a blog post on its official Medium.com page titled "DAO Maker Statement". In the blog they announced that their protocol was hacked resulting in a \$7 million loss.



DAO Maker Statement — Thursday, 12th of August



B. M. [Follow](#)

Aug 12 · 2 min read



The rapid expansion of the DAO Maker has posed several challenges to the ecosystem. These include turbulence in project onboarding and changes to company structure.

Regretfully, we must announce that in the early hours of August 12th (approx. 1 AM UTC) DAO Maker faced malicious use of one of our wallets with access to admin privileges.

The cybercriminal, after tentatively testing this exploit and managing to

Flare Token

Tuesday, September 24, 2024 11:52 AM

On 11/13/2022 blockchain auditing company Ancilia, Inc. tweeted that they detected a hack on Flare Token. They identified the attacker's address as 0xa0a613ca05daa8e8f43130a53be09bbd1a53d898.

← → ↺ x.com/AnciliaInc/status/1591849077850853378

Post

Ancilia, Inc. @AnciliaInc Follow ...

Our system detected a hack on **\$FLARE** Token. Tx: 0xa09135020bb1271ff684db407783a52163c31c7255955cec1e83fc68a751c027. Hacker: 0xa0a613ca05daa8e8f43130a53be09bbd1a53d898 withdraw almost 4B **\$FLARE** tokens and now existing via **Tornado.cash**

Transaction Hash	Method	Block	Date Time (UTC)	From	To	Amount	Token
0xa09135020bb1271ff684db407783a52163c31c7255955cec1e83fc68a751c027	Transfer	23024572	2022-11-13 16:20:36	0xa0a613ca05daa8e8f43130a53be09bbd1a53d898	Tornado.Cash.Proxy	100 BNB	BNB
0xa09135020bb1271ff684db407783a52163c31c7255955cec1e83fc68a751c027	Transfer	23024569	2022-11-13 16:20:24	0xa0a613ca05daa8e8f43130a53be09bbd1a53d898	Tornado.Cash.Proxy	100 BNB	BNB
0xa09135020bb1271ff684db407783a52163c31c7255955cec1e83fc68a751c027	Transfer	23024565	2022-11-13 16:20:15	0xa0a613ca05daa8e8f43130a53be09bbd1a53d898	Tornado.Cash.Proxy	100 BNB	BNB
0xa09135020bb1271ff684db407783a52163c31c7255955cec1e83fc68a751c027	Transfer	23024558	2022-11-13 16:25:54	0xa0a613ca05daa8e8f43130a53be09bbd1a53d898	Tornado.Cash.Proxy	100 BNB	BNB
0xa09135020bb1271ff684db407783a52163c31c7255955cec1e83fc68a751c027	Transfer	23024555	2022-11-13 16:25:45	0xa0a613ca05daa8e8f43130a53be09bbd1a53d898	Tornado.Cash.Proxy	100 BNB	BNB
0xa09135020bb1271ff684db407783a52163c31c7255955cec1e83fc68a751c027	Transfer	23024551	2022-11-13 16:25:33	0xa0a613ca05daa8e8f43130a53be09bbd1a53d898	Tornado.Cash.Proxy	100 BNB	BNB
0xa09135020bb1271ff684db407783a52163c31c7255955cec1e83fc68a751c027	Transfer	23024547	2022-11-13 16:25:21	0xa0a613ca05daa8e8f43130a53be09bbd1a53d898	Tornado.Cash.Proxy	100 BNB	BNB
0xa09135020bb1271ff684db407783a52163c31c7255955cec1e83fc68a751c027	Transfer	23024542	2022-11-13 16:25:06	0xa0a613ca05daa8e8f43130a53be09bbd1a53d898	Tornado.Cash.Proxy	100 BNB	BNB
0xa09135020bb1271ff684db407783a52163c31c7255955cec1e83fc68a751c027	Transfer	23024537	2022-11-13 16:24:51	0xa0a613ca05daa8e8f43130a53be09bbd1a53d898	Tornado.Cash.Proxy	100 BNB	BNB
0xa09135020bb1271ff684db407783a52163c31c7255955cec1e83fc68a751c027	Transfer	23024534	2022-11-13 16:24:42	0xa0a613ca05daa8e8f43130a53be09bbd1a53d898	Tornado.Cash.Proxy	100 BNB	BNB
0xa09135020bb1271ff684db407783a52163c31c7255955cec1e83fc68a751c027	Transfer	23024531	2022-11-13 16:24:33	0xa0a613ca05daa8e8f43130a53be09bbd1a53d898	Tornado.Cash.Proxy	100 BNB	BNB
0xa09135020bb1271ff684db407783a52163c31c7255955cec1e83fc68a751c027	Transfer	23024528	2022-11-13 16:24:24	0xa0a613ca05daa8e8f43130a53be09bbd1a53d898	Tornado.Cash.Proxy	100 BNB	BNB
0xa09135020bb1271ff684db407783a52163c31c7255955cec1e83fc68a751c027	Transfer	23024517	2022-11-13 16:20:51	0xa0a613ca05daa8e8f43130a53be09bbd1a53d898	Tornado.Cash.Proxy	2,000 BNB	BNB

12:42 PM · Nov 13, 2022

5 Reposts 2 Quotes 8 Likes 1 Bookmark

Most relevant

An analysis of that address on the Binance Smart Chain shows that on 11/13/2022 15:29 UTC, consistent with the Tweet, the address 0xa0a613ca05daa8e8f43130a53be09bbd1a53d898 received about 3,973,277,600 Flare tokens in txid 0xa09135020bb1271ff684db407783a52163c31c7255955cec1e83fc68a751c027.

BNB Price: \$594.40 (-0.69%) Gas: 1 Gwei

Search by Address / Txn Hash / Block / Token / Domain Name

BscScan Product of Bitfury

Home Blockchain Validators Tokens NFTs Resources Developers More Sign In

Token Transfers (BEP-20)

For 0xa0a613ca05daa8e8f43130a53be09bbd1a53d898 FLARE Token Exploiter

Sponsored: Instant Casino & Sportbooks: Get 10% Cashback and Instant Crypto Withdrawals! Play Now!

A total of 71 txns found

Transaction Hash	Method	Block	Date Time (UTC)	From	To	Amount	Token
0xd6cd92be02...	Transfer Basic...	37250328	2024-03-24 13:35:44	Big Pump: Deployer	FLARE Token Exploiter	200,000	Big Pump (PUMP)
0xb8dfc95050...	Transfer	35352704	2024-01-18 12:50:14	0x5A9b2bb5...584ed570d	FLARE Token Exploiter	13,838,686	MANTA INU (MAI)
0x6c75a08f3bc...	Transfer	23080714	2022-11-15 15:55:01	FLARE Token Exploiter	Null: 0x000...dEaD	989,000,000	Flare (FLR)
0x1119bdec30...	Transfer	23080687	2022-11-15 15:53:24	FLARE Token Exploiter	0x85AA3f04...cFE1D96A1	10,000,000	Flare (FLR)
0x01a7fc8750b...	Transfer	23080601	2022-11-15 15:48:59	FLARE Token Exploiter	0x5f054D98...30a7C5C99	1,000,000	Flare (FLR)
0x92c1e873de...	Transfer	23025868	2022-11-13 17:31:54	FLARE Token Exploiter	0x9F84A3D6...FbC848D8D	1,568,981.16161137	Binance-Peg ... (B)
0xaccfab1779...	Transfer	23025853	2022-11-13 17:31:03	FLARE Token Exploiter	0x9F84A3D6...FbC848D8D	5,975,815.1870977	Binance-Peg ... (B)

Squid Game Token

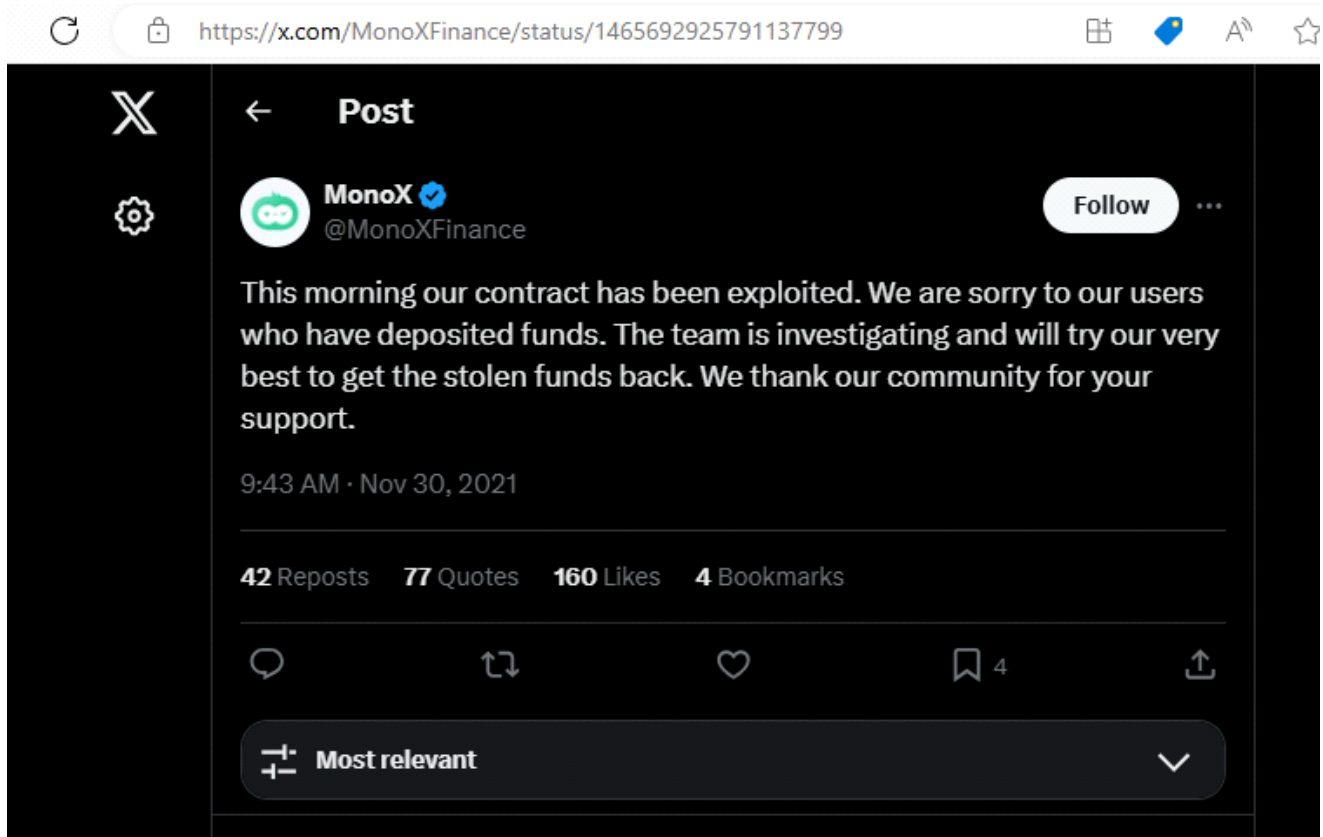
Tuesday, September 24, 2024 12:17 PM

On 11/11/2021, blockchain auditing firm sharkteam.org published a report titled "Squid game Rug pull: Fund flow analysis". In their report they describe a "rug pull" situation where the Squid game coin developers stole investor money.

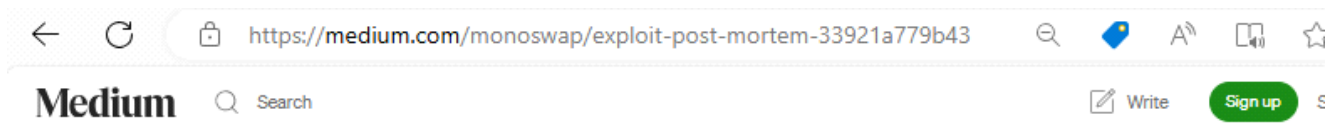
MonoX Protocol

Tuesday, September 24, 2024 12:31 PM

On 11/30/2021, MonoX tweeted from their official account that their protocol was victimized and funds were stolen:



On 12/01/2021, MonoX published a blog on their official Medium.com account titled "Exploit:Post Mortem". The blog states that approximately \$31 million in cryptocurrency was stolen.



Exploit: Post Mortem



MonoX Team · Follow

Published in MonoX · 4 min read · Dec 1, 2021



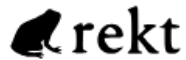
MONO Family. It's with a heavy heart that we are writing such an update.

The past 24 hours have been difficult, and we're simply at a loss for words. No apologies and no amount of words can describe how the team has been feeling since the attack transpired. We started building over a year ago with a mission to make DeFi more accessible to users and projects. We appreciate all the support we have received along the way from friends, partners, investors and our community of users.

Days like yesterday are horrible, there is no sugar coating the harsh reality of a contract being exploited and people losing money. Our supporters put their faith in a new project like us, and yesterday we let them down.

Security has always been very important to us. We conducted a three-month testnet + bug bounty, and conducted 3 audits prior to launch. In these audits,

This blog links to other published reports analyzing the mechanics of the hack. One such report is published by Rekt.news:


[T&C](#) | [Videos](#) | [leaderboard](#) | [dark](#) | [en](#)

MONOX – REKT

Tuesday, November 30, 2021

MonoX – REKT

read this article also in:

en - es - fr - ko - ru - tr - zh



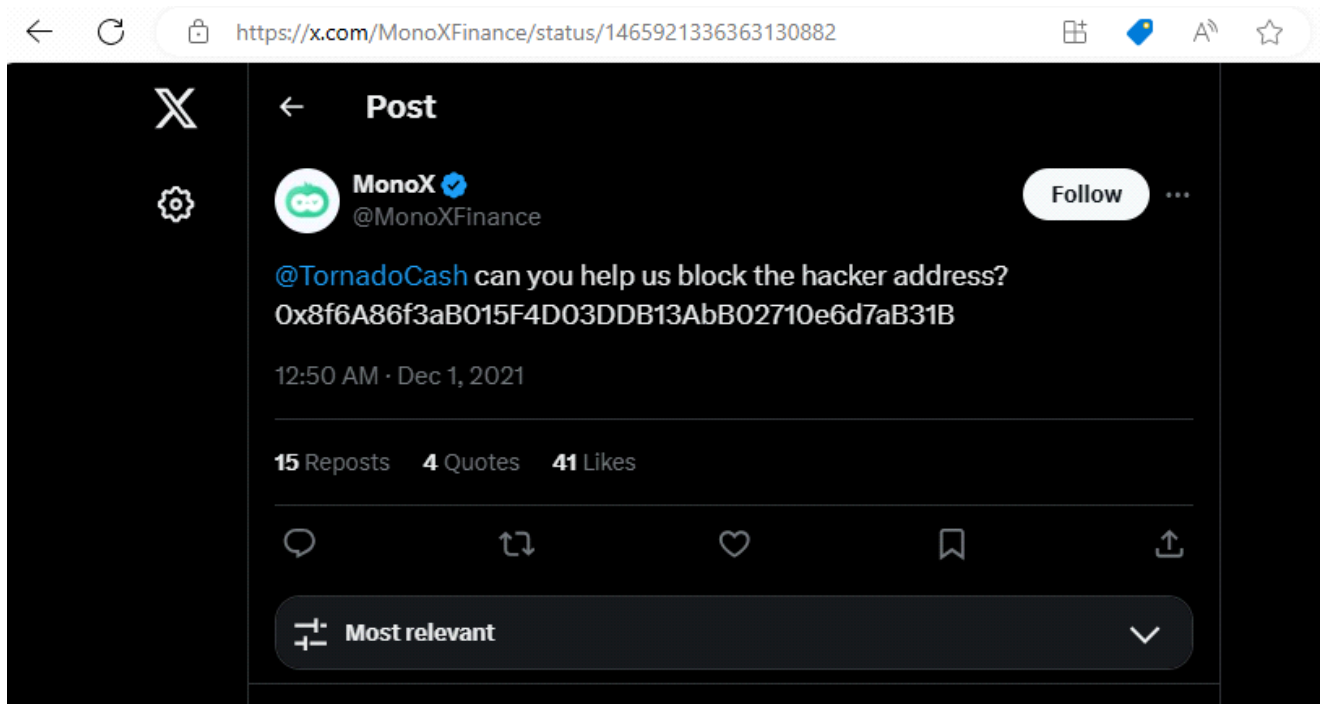
rekt by their own token.

Over \$31 million stolen, across two chains, via a price manipulation of the project's native token, MONO.

MonoX, which launched last month on Polygon and Ethereum, is a DEX based on Single Token Liquidity pools. Rather than the standard pool model of paired assets de-

The rekt report states that the stolen funds ultimately were transferred to Ethereum address 0x8f6A86f3aB015F4D03DDB13AbB02710e6d7aB31B.

This attacker address is corroborated by MonoX's official Twitter account in this tweet:



An analysis of this address shows that consistent with the Rekt report, on 11/30/2021 13:27 UTC the address received various ERC-20 tokens valued at \$11.89 million to include Wrapped Ether. On 12/01/2021 05:37 UTC, 100 Wrapped Ether is exchanged for 100 ETH deposited into this address. On 12/01/2021 05:44 UTC, 100 ETH valued at approximately \$.46 million is transferred to Tornado Cash address 0x722122df12d4e14e13ac3b6895a86e84145b6967.

Similarly, on 02/04/2022 13:21 UTC, 2,149 of Wrapped Ether is exchanged for 2,149 ETH deposited into this address. Between 02/04/2022 13:32 UTC and 02/20/2022 10:00 UTC, through a series of transactions, 2,100 ETH valued at approximately \$5.77 million is transferred to Tornado Cash address 0x722122df12d4e14e13ac3b6895a86e84145b6967.

LCX

Tuesday, September 24, 2024 1:52 PM

On 01/09/2022, cryptocurrency exchange LCX announced on their website that they suffered a hack on 01/08/2022 that resulted in a loss of approximately \$8 million.



Final Update

January 28th 2022




We are happy to announce that all deposit and withdrawal services have resumed 100% operations. Also services in collaboration with Monerium have resumed.

We would like to once again thank our clients, customers, partners, and the broader crypto community for your support during this period.

In this report they detail that the address that received the stolen funds was:
0x165402279f2c081c54b00f0e08812f3fd4560a05.

← ↻ 🔒 <https://www.lcx.com/hot-wallet-incident-report/> 🔊 📄 ☆ ...

And lastly, we also continue to work with authorities and external cyber security firms. Additional details will be published here.

Update January 9th, 2022

At roughly 11:23 PM CET on January 9th, LCX's Technology team detected unauthorized access of one crypto wallet at the LCX platform. A total of approx. 7.94M USD of crypto assets were stolen. 0.70M USD have been frozen. All other LCX wallets are not impacted.

During this difficult period we greatly appreciate the support from our customers, other exchanges, security experts, and the broader crypto community. LCX will continue to do everything in its power to mitigate the impact from this incident and restore full service as soon as possible.

Incident Details

The hacker wallet address is [0x165402279f2c081c54b00f0e08812f3fd4560a05](#).

The theft took place yesterday evening, January 8th 2022 between 11:23 PM and 11:37 PM CET.

During this period, the following cryptocurrencies were stolen:

Cryptocurrency (approx. USD value according to Coingecko):

- 162.68 ETH (502,671 USD)
- 3,437,783.23 USDC (3,437,783 USD)
- 761,236.94 EURE (864,840 USD)
- 101,249.71 SAND Token (485,995 USD)

An analysis of the hacker's address shows that consistent with the details publicly reported by LCX, between 01/08/2022 22:23 UTC and 22:35 UTC, various ERC-20 tokens were transferred from a wallet associated with LCX.

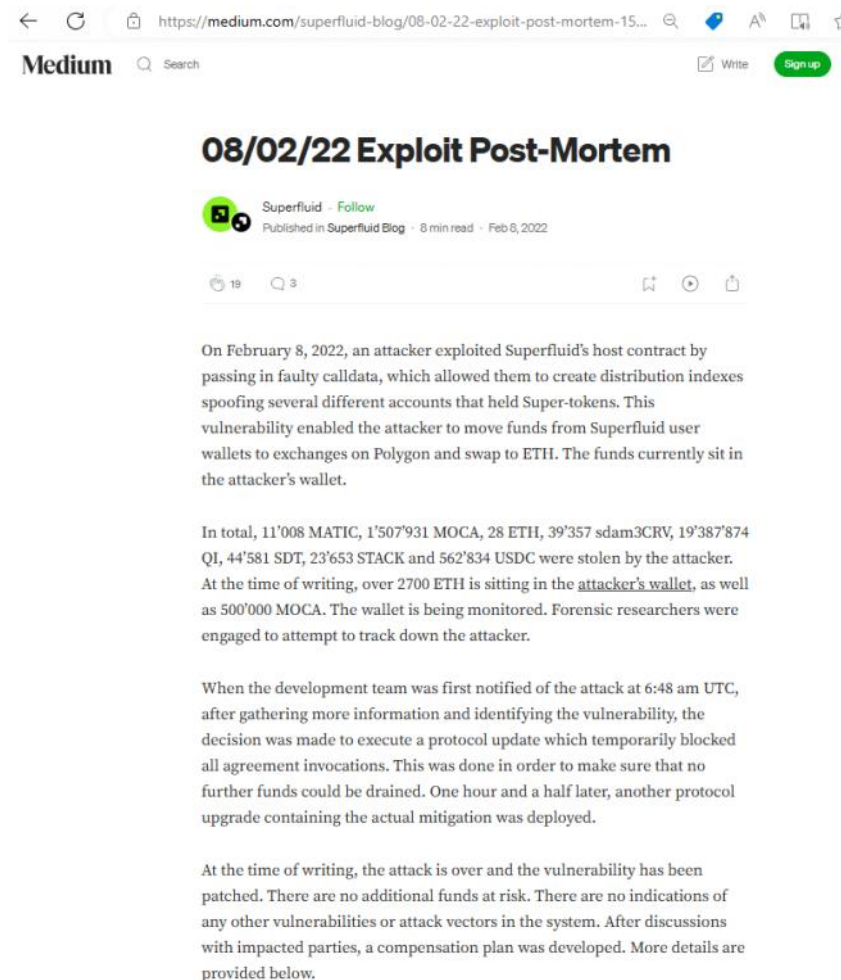
Also, on 01/08/2022 between 22:26 UTC and 22:37 UTC, about 162 ETH valued at approximately .43 million was transferred from an address associated with LCX to the hacker's wallet.

The ERC-20 tokens were then swapped between 01/08/2022 22:40 UTC and 01/10/2022 20:29 UTC for ETH.

Superfluid

Tuesday, September 24, 2024 2:28 PM

On 02/08/2022, Superfluid published a blog post on their official account on Medium.com titled "08/02/22 Exploit Post-Mortem". This post stated that on 02/08/2022 an attacker exploited Superfluid's protocol and was able to steal cryptocurrency.



Medium Search Write Sign up

08/02/22 Exploit Post-Mortem

Superfluid · Follow
Published in Superfluid Blog · 8 min read · Feb 8, 2022

19 3

On February 8, 2022, an attacker exploited Superfluid's host contract by passing in faulty calldata, which allowed them to create distribution indexes spoofing several different accounts that held Super-tokens. This vulnerability enabled the attacker to move funds from Superfluid user wallets to exchanges on Polygon and swap to ETH. The funds currently sit in the attacker's wallet.

In total, 11'008 MATIC, 1'507'931 MOCA, 28 ETH, 39'357 sdam3CRV, 19'387'874 QI, 44'581 SDT, 23'653 STACK and 562'834 USDC were stolen by the attacker. At the time of writing, over 2700 ETH is sitting in the attacker's wallet, as well as 500'000 MOCA. The wallet is being monitored. Forensic researchers were engaged to attempt to track down the attacker.

When the development team was first notified of the attack at 6:48 am UTC, after gathering more information and identifying the vulnerability, the decision was made to execute a protocol update which temporarily blocked all agreement invocations. This was done in order to make sure that no further funds could be drained. One hour and a half later, another protocol upgrade containing the actual mitigation was deployed.

At the time of writing, the attack is over and the vulnerability has been patched. There are no additional funds at risk. There are no indications of any other vulnerabilities or attack vectors in the system. After discussions with impacted parties, a compensation plan was developed. More details are provided below.

In the blog post, the hacker's Polygon address was identified as 0x1574F7F4C9d3aCa2EbcE918e5d19d18aE853c090.

An analysis of this address shows that consistent with the post-mortem, the address received various tokens on 02/08/2022 6:17 UTC.

Hundred Finance

Tuesday, September 24, 2024 3:26 PM

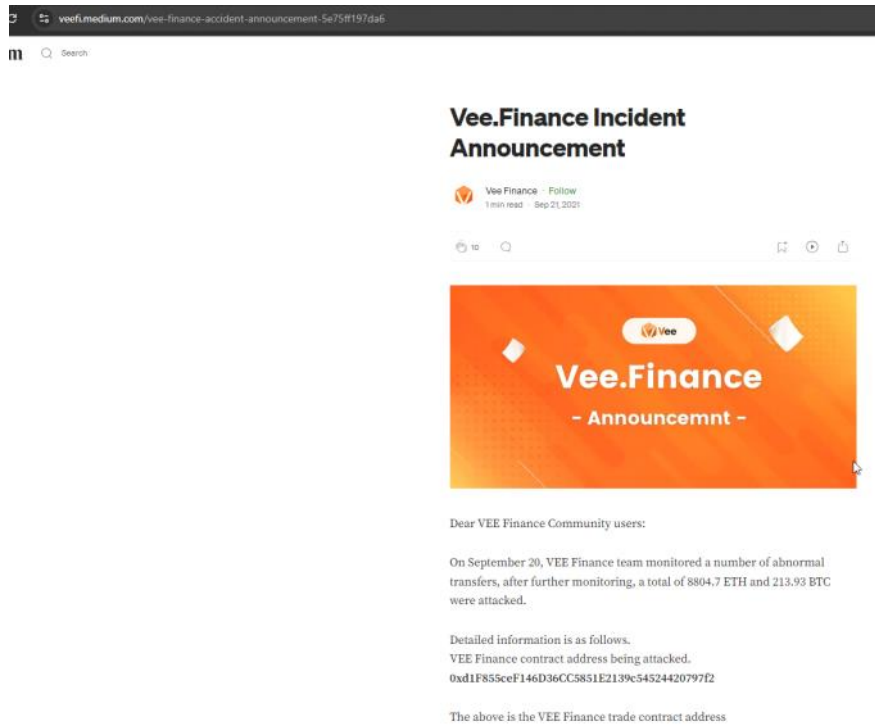
On 03/15/2022, Hundred Finance confirmed on their official Twitter account that they had been hacked:



Vee Finance

Tuesday, September 24, 2024 3:36 PM

On 09/21/2021, Vee Finance announced via a blog post on their official Medium.com account that they had been hacked on 09/20/2021.



In this post they detail that various cryptocurrencies had been stolen and transferred into the attacker's address: 0xeeee458C3a5eaAfcFd68681d405fB55eF80595BA

Analyzing this address show that consistent with the blog post, between 09/20/2021 20:49 UTC and 09/21/2021 07:03 UTC, this address received a large amount of Wrapped BTC and Wrapped ETH.

On 09/22/2021 21:54 UTC, the hacker converted the Wrapped ETH to Ether, netting approximately 8,804 ETH valued at about \$23.28 million.

<https://etherscan.io/address/0xeeee458c3a5eaafcd68681d405fb55ef80595ba#internaltx>

The screenshot shows the Etherscan.io interface for the address 0xeeee458c3a5eaafcd68681d405fb55ef80595ba. The "Internal Transactions" tab is selected, showing a list of 4 latest internal transactions. The table below summarizes these transactions:

Parent Transaction Hash	Block	Date Time (UTC)	From	To	Amount
0xa23dc9d618...	13278113	2021-09-22 21:54:01	Wrapped Ether	Vee Finance Exploiter	8,803.70733248 ETH
0x34b1765ee7...	13264408	2021-09-20 19:05:00	Tornado.Cash: 10 ETH	Vee Finance Exploiter	9.9492617 ETH
0x3e25d185a7...	13264395	2021-09-20 19:01:37	Tornado.Cash: 10 ETH	Vee Finance Exploiter	9.9630833 ETH
0x1faa95fa7a5...	13264383	2021-09-20 18:58:52	Tornado.Cash: 10 ETH	Vee Finance Exploiter	9.9627791 ETH

Between 09/22/2021 22:06 UTC and 09/22/2021 23:13 UTC, the hacker sent about 8,806 ETH to address 0xEe33902b81eb4b4A6988E84Ebbf7E9A72fd2E0B6.

Saddle Finance

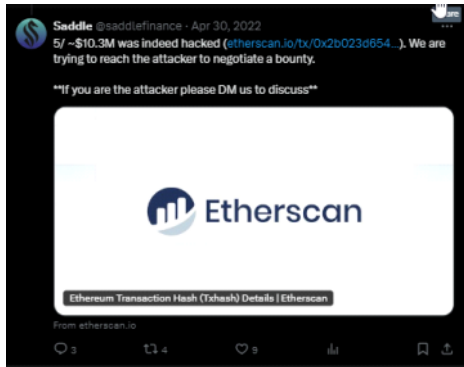
Tuesday, September 24, 2024 5:03 PM

On 04/30/2022, Saddle Finance announced via Twitter that their protocol had been hacked:



In another Twitter post, Saddle Finance states that \$10.3 was hacked and they shared the Ethereum transaction associated with the hack:

0x2b023d65485c4bb68d781960c2196588d03b871dc9eb1c054f596b7ca6f7da56



On 05/03/2022, Saddle Finance published a now deleted blog on their website titled "Post-mortem of Mainnet sUSDv2 metapool exploit":



4/30/2022: Post-mortem of Mainnet sUSDv2 metapool exploit

UPDATE: Figures for exploit amount rectified to reflect total amount hacked.

On 4/30/2022, the **sUSD metapool on Mainnet** was exploited for \$11.9m due to a vulnerability resulting from reusing an incorrect library deployment.

Because of the vulnerability, a malicious blackhat hacker was able to use a flash loan attack to drain \$11.9m in funds from the sUSDv2 metapool.

The total amount of funds drained would have been greater. However, \$3.97m was secured by **BlockSec**, a whitelhat security firm. By using an internal bot that detects and tracks hacking activities on the blockchain, BlockSec was able to frontrun the theft of an additional \$3.97m by the attacker. In addition, due to rapid response to the incident, the attack affected only one of three pools that were vulnerable to this exploit.

Upon learning of the exploit, Saddle immediately paused all pools. On 5/2/2022, Saddle pushed out a fix for the vulnerability. Today, Saddle is **resuming metapool operations for unaffected pools**, as detailed below:

- Arbitrum USDs (Sperax) metapool - unaffected by vulnerability - Same pool is resumed
- Evmos tBTC metapool - unaffected by vulnerability - Same pool is resumed

We're pushing new contracts with the fix for the affected pools, which will be deployed later this week as new pools.

The team is also continuing work on remuneration plans for affected LPs, a bounty of ~\$400K to BlockSec (pending [governance vote](#)), and implementing additional security and monitoring measures. Read on to learn more.

The post-mortem identifies two malicious transactions that drained the protocol of approximately \$11.9 million in cryptocurrency.

The two malicious transactions were identified as:

<https://etherscan.io/tx/0x2b023d65485c4bb68d781960c2196588d03b871dc9eb1c054f596b7ca6f7da56>


<https://etherscan.io/tx/0xe7e0474793aad11875c131ebd7582c8b73499dd3c5a473b59e6762d4e373d7b8>

An analysis of these transactions show that they were both ordered by address 0x633418a917De90498F3903B199Df5699b4a55AC0.

Harmony Horizon Bridge


Tuesday, September 24, 2024 5:30 PM


On 08/01/2022, Harmony published an article on their official website titled "Summary of the Horizon Bridge Incident". In the article they detail that they suffered an exploit on 06/23/2022 resulting in the loss of cryptocurrency. The article also identifies the hacker's Ethereum account: 0x0d043128146654C7683Fbf30ac98D7B2285DeD00


[Funding](#)
[Community](#)
[Governance](#)
[Web3](#)
[Res](#)

Summary of the Horizon Bridge Incident

Community Announcements


Jacksteroo OP ⚡
1 Aug 2022



An individual, group or groups of perpetrators began transferring Harmony's Horizon Bridge's assets on the Ethereum chain, starting on **Jun-23-2022 11:06:46 AM +UTC** ¹⁵, 14 bridged assets, including USDC, ETH and USDT on Ethereum, and also BNB on Binance Smart Chain, into a previously unrecognized account **0x0d04...d000** ⁸. The perpetrator(s) compromised at least two out of four private keys of the bridge validators and gained control of the bridged assets, to then begin funneling the assets into a combination of new wallets (known as wallet hopping) and eventually into a mixer called Tornado Cash. Forensics teams are actively monitoring the activities of these wallets and the mixer.

Harmony had offered a \$1M bounty to return the remaining stolen amount. The bounty was soon after **increased to \$10M** ¹⁸ but Harmony has not received a legitimate response to date. The global hunt continues with investigations passed on to the Federal Bureau of Investigation (FBI) with the cooperation of partners, including multinational cryptocurrency exchanges. We believe

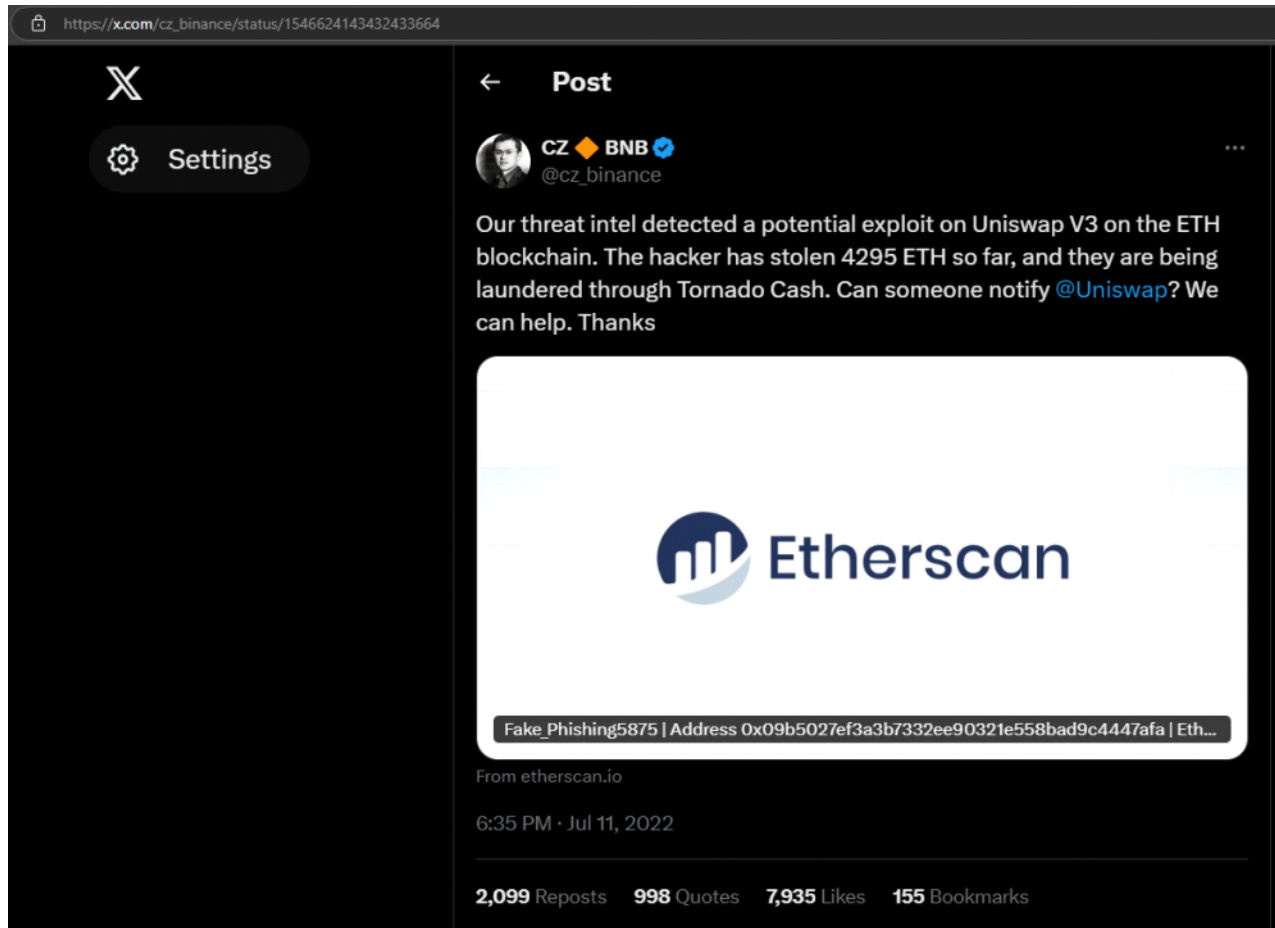
An analysis of the hacker's address shows that consistent with the incident summary, between 06/23/2022 11:08 UTC and 06/23/2022 11:26 UTC a large amount of ERC20 tokens were transferred from the Harmony Bridge. These tokens were swapped for Ether.

Between 06/27/2022 07:10 UTC and 07/01/2022 15:45 UTC, wallet 0x0d043128146654C7683Fbf30ac98D7B2285DeD00 transferred 85,866 ETH to five intermediary

Uniswap Phishing

Saturday, October 19, 2024 7:42 PM

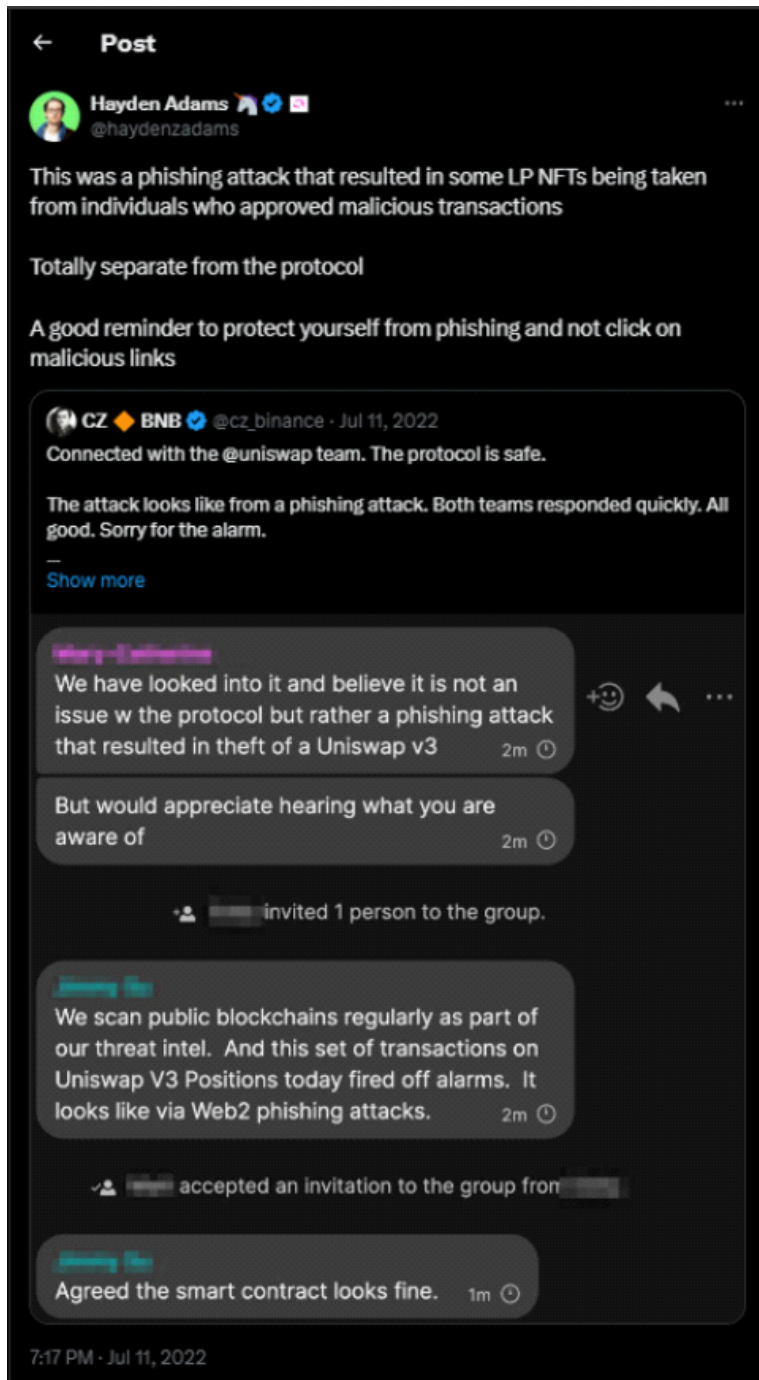
On July 11, 2022, the CEO of Binance Changpeng Zhao tweeted that there was a potential exploit with Uniswap and that Ether was being transferred to wallet 0x09b5027eF3a3b7332EE90321E558baD9C4447AFA:



The next day this was corroborated in a Tweet from Uniswap Labs:



Hayden Adams, the creator of Uniswap responded to CZ's tweets on the subject stating:




An analysis of Ethereum address 0x09b5027eF3a3b7332EE90321E558baD9C4447AFA shows that indeed it received about 240.41 Wrapped BTC on 07/11/2022 from an Ethereum address associated with Uniswap.

Crypto.com

Saturday, October 19, 2024 8:29 PM

On 01/20/2022 bitcoin exchange Crypto.com announced on their website that they had been hacked on 01/17/2022.

https://crypto.com/product-news/crypto-com-security-report-next-steps

crypto.com |  Download App

Summary

On 17 January 2022, Crypto.com learned that a small number of users had unauthorized crypto withdrawals on their accounts. Crypto.com promptly suspended withdrawals for all tokens to initiate an investigation and worked around the clock to address the issue. No customers experienced a loss of funds. In the majority of cases we prevented the unauthorized withdrawal, and in all other cases customers were fully reimbursed.

The incident affected 483 Crypto.com users.

Unauthorised withdrawals totalled 4,836.26 ETH, 443.93 BTC and approximately US\$66,200 in other cryptocurrencies.

What happened?

On Monday, 17 January 2022 at approximately 12:46 AM UTC Crypto.com's risk monitoring systems detected unauthorized activity on a small number of user accounts where transactions were being approved without the 2FA authentication control being inputted by the user. This triggered an immediate response from multiple teams to assess the impact. All withdrawals on the platform were suspended for the duration of the investigation. Any accounts found to be impacted were fully restored. Crypto.com revoked all customer 2FA tokens, and added additional security hardening measures, which required all customers to re-login and set up their 2FA token to ensure only authorized activity would occur. Downtime of the withdrawal infrastructure was approximately 14 hours, and withdrawals were resumed at 5:46 PM UTC, 18 January 2022.

On 08/19/2022, blockchain forensics firm SlowMist released their 2022 Mid-Year Report on Blockchain Incidents and Methods of Laundering. In their report, they identify the Crypto.com hacker's Ethereum address as 0x6e1218c55f1aCb588Fc5E55B721f1183D7D29D3d:

https://medium.com/coinmonks/2022-mid-year-report-on-blockchain-l...

- Crypto.com

Hackers Addresses:

0x6e1218c55f1aCb588Fc5E55B721f1183D7D29D3d (ETH)

bc1qk8wlpvvr6v5lmsngg5a248k2a9cgrsrw5jsq (BTC)

bc1q83c9e7s8925hhy9dqpdyfctgwaspj3wdrhqr (BTC)

bc1qk7e2k8s252789cggr5xy67m6jvc0jsqpdjfw9d (BTC)

bc1qnzn9wmt40qwuhd7zmqvmvd0c3zazv59ljplnr (BTC)

bc1qy7hf94vv20jqez2fk8xyxuv0h0u8r0kh8cau46 (BTC)

Date: 01/17/2022, 01/18/2022

Amount: 4,836.2596 ETH, 443.9322 BTC

InitialFunding: N/A

Event:



(Crypto.com Hacker — Timeline of Fund Transfers)